VTT Technical Research Centre of Finland

Advanced technologies for productivity-driven lifecycle services and partnerships in a business network

Ahonen, Toni

Published: 07/10/2019

Document Version
Publisher's final version

RESEARCH REPORT

VTT-R-00954-19

TecNetwork

Advanced technologies for productivity-driven lifecycle services and partnerships in a business network

Authors: Toni Ahonen, Jari Ahola, Pekka Isto, Mikaela Ranta, Timo Malm, Tero Välisalo, Esko Strömmer, Antti Tanskanen, Arto Ylisaukko-oja, Markku Järviluoma, Pekka Kilpeläinen, Tuomas Seppälä, Pentti Vostrakov, Severi Olsbo, Esa Viljamaa, Jukka Koskinen, Janne Saukkoriipi, Tapio Heikkilä

Confidentiality: Public

VTT

Report's title

Advanced technologies for productivity-driven lifecycle services and partnerships in a business network

Customer, contact person, address	**Order reference**
Business Finland	7289/31/2016
Project name	**Project number/Short name**
Advanced technologies for productivity-driven lifecycle services and partnerships in a business network	TecNetwork
Author(s)	**Pages**
Toni Ahonen, Jari Ahola, Pekka Isto, Mikaela Ranta, Timo Malm, Tero Välisalo, Esko Strömmer, Antti Tanskanen, Arto Ylisaukko-oja, Markku Järviluoma, Pekka Kilpeläinen, Tuomas Seppälä, Pentti Vostrakov, Severi Olsbo, Esa Viljamaa, Jukka Koskinen, Janne Saukkorlipi, Tapio Heikkilä	79
Keywords	**Report identification code**
Digitalization, automation, safety, productivity, services	VTT-R-00954-19

Summary

The TecNetwork project has aimed at fostering the development of new solutions for the underground mining sector that exploit the emerging opportunities of Industrial Internet technologies and address the new requirements for digitalizing processes, electrification and goals for safe and sustainable operations. Furthermore, the research themes of the project have been selected so that they support the development of novel industrial services in a wide spectrum of industries.

Resource scarcity, growing awareness of environmental issues and demand for more efficient processes are drivers for machine and equipment manufacturers' new offerings. The goal of TecNetwork was to support machine and production system providers and their ecosystem partners in creating new offerings with safer and sustainable processes that meet the changing requirements of the business environment.

TecNetwork project is divided into four research topics:

- Industrial Internet solutions for safety and productivity in underground mining
- Securing machine safety
- Management of electric fleets in modern underground mines
- Control system development towards autonomous machines and processes

Furthermore, the project has explored how an ecosystem should collaborate and develop services enabled by digital technologies, aiming at new business opportunities in full-line underground mining services.

The report presents the progress achieved in the above-mentioned topics in the TecNetwork project. Summaries of the topics are provided at the beginning of each section.

Confidentiality	Public

Tampere 7.10.2019

Written by	**Reviewed by**	**Accepted by**
Toni Ahonen	Aki Aapaoja	Tiina Valjakka

VTT's contact address

Vuorimiehentie 3, Espoo / PO 1000, 02044 VTT

Distribution (customer and VTT)

2 pcs (project manager, VTT archive), PDF-version at the project website

Preface

This final report of the TecNetwork project collects the core findings of the project.

This report has been written by a number of experts from VTT. *In Section 2* the results regarding the research on UWB positioning are written by Pentti Vostrakov, Severi Olsbo and Esa Viljamaa, and Wired Ethernet connectivity has been addressed by Pekka Isto. Esko Strömmer, Antti Tanskanen and Arto Ylisaukko-oja have presented the research results and applications of cable-free power and communication.

Section 3 introduces automation development towards autonomous machine systems. The presented roadmap towards autonomous mobile machines is authored by Jari Ahola, Tapio Heikkilä, Pekka Isto and Markku Järviluoma. The topics related to computer-assisted control and autonomic features, namely collision-free path planning and boom deflection modelling, were studied and reported by Jari Ahola, Tuomas Seppälä, Jukka Koskinen, Janne Saukkoriipi and Pekka Isto.

Timo Malm, Tero Välisalo and Toni Ahonen are responsible for the topics in *Section 4* introducing new information related to securing machine safety.

Section 5, written by Toni Ahonen, introduces the results of the TecNetwork project on business ecosystem development and joint industrial service business development.

Section 6, introducing a tool for the simulation and management of an electric machine fleet, is written by Mikaela Ranta.

The authors gratefully acknowledge Business Finland for funding the research project and the companies involved in the research. Our acknowledgements also go to the members of the project's steering group and the following colleagues for their valuable support during the project: Aki Aapaoja, Esa Viljamaa, Mikko Pihlatie, and Karoliina Salminen.

Tampere 7.10.2019

Authors

Contents

1. Introduction

Development cycles, business logics and requirements for effectiveness over asset lifecycles have been undergoing changes in recent years in the mining and construction sectors. This has led to structural changes that will also strongly affect the role of service providers. Interest towards digital services has increased, while customers are also willing to buy effectiveness and easiness for their operations at a competitive price. Furthermore, fleet management and consideration of the whole lifecycle of assets are having an increasing role.

Resource scarcity, growing awareness of environmental issues and demand for more efficient processes are drivers for the creation of new offerings by machine and equipment manufacturers. The TecNetwork project has targeted improving the productivity of industrial processes by creating new technological capabilities in selected potential areas and considering cost-efficiency, availability performance, safety, and smart decisions throughout the lifecycles of assets. The research results produced will support machine and production system providers in creating new offerings with safer and sustainable processes that will meet the changing requirements of the business environment.

The TecNetwork project covers development areas at the business, process and technology levels, creating novel technology solutions, approaches for utilizing digital tools, new knowledge of safety solutions, and applications for analysing the value of emerging business models. Companies are seeking better control and management of work processes to improve the productivity, safety and utilization of machinery and to manage and optimize lifecycle costs. Continuous automated work processes with novel technologies for data gathering, analytics and management as well as for connectivity and control are of increasing interest. Modern mobile work machines are demanded to be safe, efficient and ecological, which further increases demand for new solutions and R&D work.

Reliability, utilization rate and quality, alongside improvements in equipment production capacity and risk management, are crucial factors in ensuring the competitiveness of the capital-intensive industry. The expectations towards asset management are changing: instead of separate technical solutions, companies want to have comprehensive methods and tools that bring assessment, planning, development, and optimization as well as technical, organizational and economic perspectives together. Regarding the value-based management of assets, the trends and drivers shown in Figure 1 can be identified with respect to the project research themes.

The TecNetwork project is divided into four research themes, as shown in Figure 1. The research areas for each of the themes are selected based on the long-term needs of industrial ecosystems.

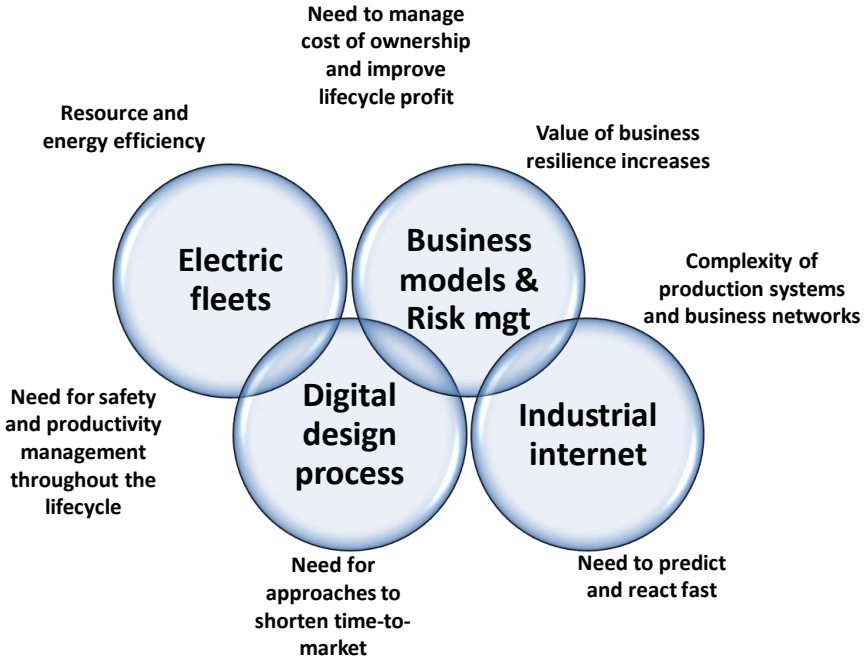


Figure 1. *Trends and drivers.*

Industrial Internet: The Industrial Internet technologies addressed in this project cover (1) Wireless solutions for safety and asset management, (2) Wired Ethernet connectivity and (3) Cable-free power and communication. Furthermore, analytics integration capabilities with respect to O&M analytics are addressed in the 'Digital design process' theme. The project will create novel solutions within these areas, and where relevant, solve the bottlenecks and shortcomings of recent solutions.

Business and system risks and opportunity management: Provision of novel full-line services in a networked environment requires new understanding of the management of the network and adoption of new business models for the network. The project considers a techno-economic model for the management of assets, which will provide a baseline for creating suitable business models for the provider network. A design process for considering safety, security and reliability in a holistic manner will be created.

Electric fleets: Electrification of vehicles and machinery, already taking place on the public transport side, is an emerging opportunity. The project addresses the entire design process for electric vehicles or machinery. Previous models will be supplemented with consideration of optimization functions for fleets, energy and total cost of ownership.

Digital design process: The emphasis of the work has been on creating capabilities that will be required in the future when designing autonomous systems. This development will happen in phases, which have been analysed by VTT, and is also addressed as a roadmap in this report.

2. Industrial Internet solutions

The TecNetwork Industrial Internet research theme consists of the following three sub-topics:

- Wired Ethernet connectivity
- UWB positioning solutions for safety and asset management
- Cable-free power and communication

The Ethernet is the network technology of choice for office and telecom environments and it is fast being adapted also in the automotive industry. Ethernet is expected to become the high-bandwidth network backbone of vehicles as high data volume sensors such as surround-view cameras, 3D scanners and radars, and other systems supporting ADAS will overtax FlexRay.

In modern mining and tunnelling applications, safety is the number one priority. Autonomous mining is also challenging the current safety solutions in place for operating environments, personnel and devices. Autonomous movement of working machines must be restricted with safety sensor solutions and remote tools and components must be positioned and identified more accurately. Less manpower combined with more autonomous tasks means less human peer observation and less human help in the event of accidents. Autonomous machine environment safety solutions have been traditionally based mostly on restricted working areas and dedicated sensing solutions attached to machines. There is plenty of room for new safety and asset management solutions in mining processes involving semi-autonomous and autonomous machines. The TecNetwork project brought ultra-wideband (UWB) based communication and positioning technology under closer examination in the mining safety and asset management context.

Wireless sensors and actuators are becoming more and more common due to the development trend of the Internet of Things (IoT). In many cases it is not possible to use cables for powering and communications, for example due to installation costs or the mechanical structure of the surroundings (e.g. rotating machine parts). Even though several technology options for low-power wireless communication are available, powering by battery may be inconvenient or a considerable cost factor over the lifecycle of wireless IoT devices in professional applications, since the battery typically requires manual replacements or recharging even if the energy consumption of the IoT device is optimized. The goal in this project was to further develop a previously developed preliminary approach for better performance and wider application potential of wireless and batteryless IoT nodes with UHF (Ultra-High Frequency) radio based powering and communication.

2.1 Wireless solutions for safety and asset management with UWB

Positioning is the process of determining positions of people, equipment, and other objects. Positioning can be classified into real-time locating systems (RTLS) and global positioning systems (GPS) depending on the environment in which the positioning is conducted: indoors or outdoors. Different applications may require different types of positioning technologies that fit their needs and constraints. For example, Global Positioning System (GPS) technology is efficient only for outdoor spaces because satellite radio signals cannot penetrate solid walls or obstacles [Sensors 2016, https://www.mdpi.com/1424-8220/16/5/707/htm].

RTLS determines the position of an object in a physical space continuously and in real-time. It uses numerous positioning approaches, which vary greatly in terms of accuracy, cost, precision, technology, scalability, robustness and security. Indoor positioning has its own requirements that differentiate it from outdoor positioning. There are five main quality metrics of indoor positioning systems: (1) system accuracy and precision; (2) coverage and its resolution; (3) latency or frequency in making location updates; (4) building's infrastructure impact; and (5) effect of random errors on the system, such as errors caused by signal interference and reflection [Sensors 2016]. Not all of these quality metrics are considered in the performed measurements described later. Ultra-wideband (UWB) positioning systems are classified as real-time locating systems (RTLS).

RTLSs are used to automatically identify and track the location of objects or people in real time, usually within a building or other contained area. Wireless RTLS tags are attached to objects or worn by people, and most RTLSs work according to a relative coordinate system of fixed reference points that receive wireless signals from tags to determine locations.
Nowadays mines depend on cell-based Wi-Fi network location with an accuracy of around 50 metres. In addition, RFID tags are used to located people and vehicles in the mine. However, this is very inaccurate and the location is not known in real-time. GPS cannot be used in underground mines because the signal is available only above ground.

In VTT's UWB positioning system, location is determined by measuring the distance between radio transmitters and receivers using the time difference of arrival method (TDOA). UWB radio operates at around 5 GHz frequency with 500 MHz bandwidth, which gives it unique advantages over narrowband signals. The wide bandwidth can go through walls more easily, is immune to multipath fading, and is not interfered by signals from other devices. Instead of continuous waveform transmission, UWB uses sub-nanosecond pulses to send information, which can provide high precision TDOA calculations that are not possible with narrowband radios. In TDOA measurement, at least three base stations are needed for location calculation.

VTT's current location system, further developed and applied in the TecNetwork project, consists of at least one master base station (MBS) for time sync and communications, two base stations (BS) for location, and a battery operated location receiver (TAG). Up to eight base stations are supported by one MBS, each improving the coverage and location accuracy of the network. With multiple MBSs, the network can be expanded in multi-cell mode where all MBS's are connected together via IP network. Calculating the location from TDOA measurements is made in the location TAG device, so connections to external servers is not required and location can be used in the TAG, similar to a GPS receiver but in relative coordinates. Currently, one multi-cell network supports 600 TAG devices locating once per second.

BS and TAG have identical hardware, whereas MBS has a different processor but the same radio. It could be possible to use same hardware in MBS as in TAG and BS.

2.1.1 A test for accuracy and applicability of UWB positioning

To test the applicability of UWB positioning, a test network was built and a precision GPS handheld device Zeno 20 UMTS made by Leica was used to produce reference location data. The UWB test network was implemented as a one-cell construction in the middle of a sports area approximately 80x140 metres in size (large football field). No large buildings or trees were in the near proximity, ensuring practically zero reflection of UWB radio signals.
The network consisted of a master base station (MBS) and eight base stations (BS) as shown in the figure below. The bottom left corner was selected as the origin with BS1 as the zero point. The MBS was located inside the cell. One TAG was to be located in the UWB network.

The TAG to be located within the UWB system was tied together with the GPS receiver. The ‘receiver package’ was positioned so that the devices were located in relation to each other and parallel to the X-axis of the UWB coordinates. The height of the receiver package from the ground was 1.5 metres. Both systems updated the location once a second and were not synchronized – which causes difference in results. The difference was not compensated in any way.

Locations given by GPS were converted from WGS-84 to Cartesian coordinates and transformed to the UWB network’s coordinate system with known reference point. The receivers were moved by slowly pacing out a circle, which in practice was an oval (Figure 2), and a square (Figure 3). The walking speed was determined to be around 0.6 metres per second.

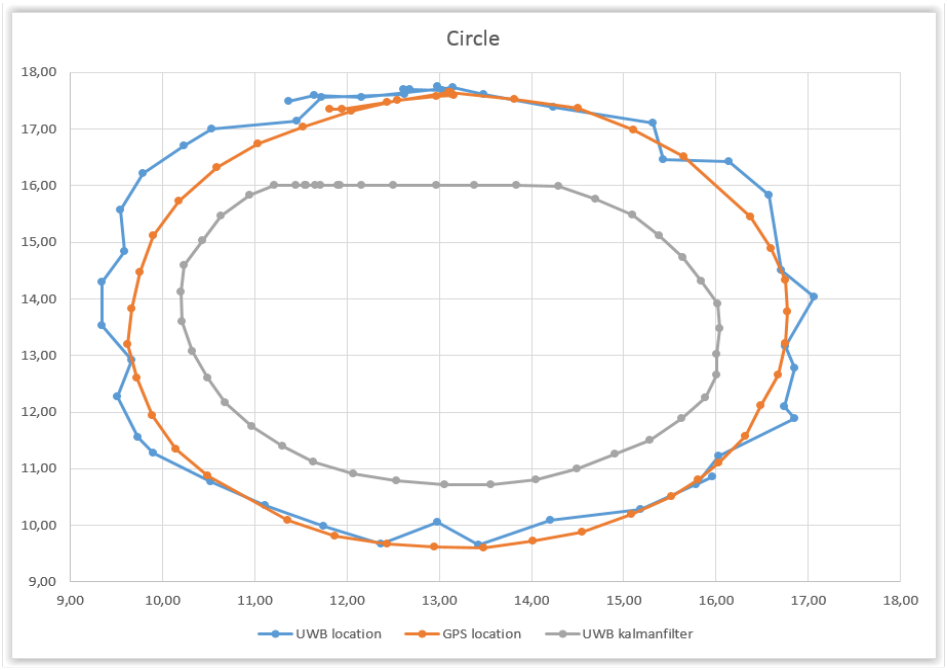


Figure 2. *Test results for an oval.*

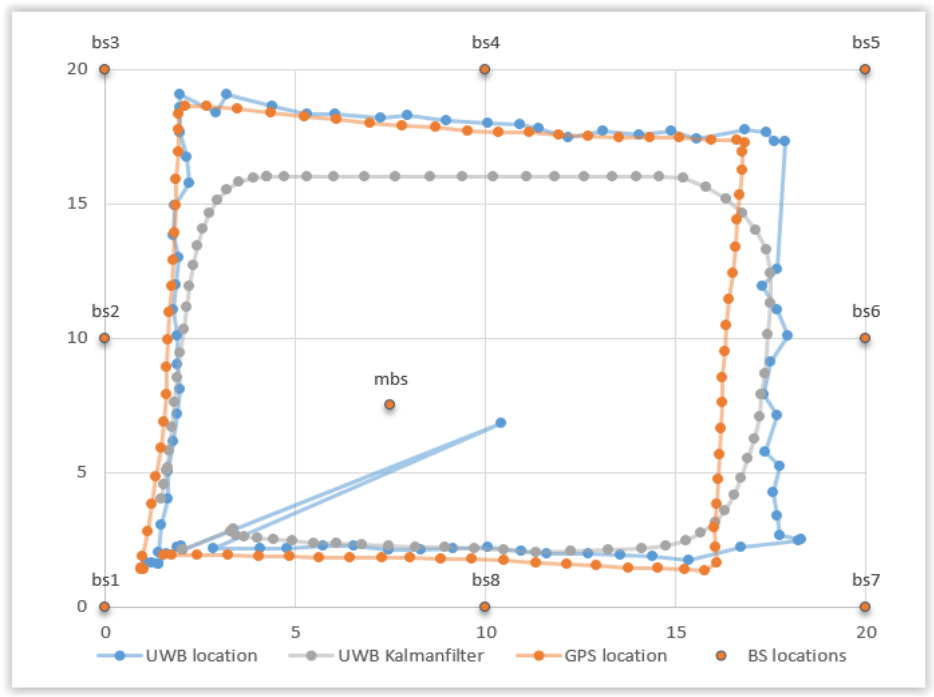


Figure 3. *Test results for a square.*

During the measurements it was noticed that the TAG did not always fully hear the BSs. The reason was found to be the low transmission power of one the BSs, which had been configured for indoor use. There were no intervening obstacles.

As can be seen from the figures above, the raw UWB location is mainly nearer the GPS location than the UWB location using the Kalman filter. In the oval, the difference between the unfiltered UWB and GPS location is more or less random, with a median of 39 cm and 90% within 73 cm, while in the square, the median is 1.23 metres and 90% is under 2 metres. Three sides of the square have quite similar values, but on one side the difference is clear and quite uniform in the X-axis. On one side of the square (top), the Kalman filter gives the respective difference, but now in the Y-axis. The Kalman filter seems to round the corners of the square.

In the oval, the Kalman filter gives a smaller movement (smaller oval) and the uniform average difference is 1.1 metres, as can be clearly seen in the figure. With Kalman filtering applied, erratic fluctuations of raw UWB TDOA calculations are smoothed out in both tests except at the top of the oval, where the locations form a straight line with a bigger difference in Y-coordinates compared to other parts of the oval. The Kalman filter for some unknown reason restricts the Y-axis value to 16, as is visible in both diagrams.

2.1.2 Test summary

Most of the standard error between the GPS and UWB systems in the tests is due to timing error between the location systems. The GPS receiver used could not provide a time sync signal to synchronize the UWB position.

Another source of error was inaccurate BS locations. The current UWB system requires surveying positions for each BS and MBS and, as seen in the field tests, this can be problematic when there are no structures to install the BS to.

VTT UWB system is originally intended for indoor use. For outdoor uses, the specific purpose of use should be analysed and any required changes made to the system accordingly.

2.1.3 Commercial UWB systems

Real-Trac has developed an underground UWB positioning system for mines that allows tracking within one metre radius. Location tags are built in to the headlamps to alert personnel of a hazard with flashing lights and vibrations, or within vehicles and machinery by alerting drivers with a proximity display. The Real-Trac system can also provide communications and telemetry with a UWB network. [https://real-trac.com/en/]

Sewio Networks is manufacturer of indoor UWB systems and provides extensive industrial productivity analysis software with their RTLS platform. [https://www.sewio.net/]
One of larger UWB device producers is company called Ciholas. They have long record of creating custom hardware based around Decawave DWR1000 UWB transmitters and selling commercial indoor location systems. One of the largest installations made by Ciholas covers a 43 000 m2 museum. They developed a new proprietary location algorithm to mitigate and detect obstructed UWB signals inside the museum. Their system relies on external servers located in the basement thus limiting the capacity of the system to serve a high number of locatable devices. [https://www.ciholas.com/]

It seems that Decawave UWB radios are currently most popular in commercial systems due to their low price and ease of use.

First introduced in 2006, the IEEE 802.15.4 standard defines physical and media access (MAC) layers for UWB and support for ranging capabilities.

The new IEEE 802.15.4z standard will specify more strict security for physical layer (PHY) and MAC layers than the previous version. A draft of the standard was released 4/2019. More secure standards are required for location-based authentication as used in cars and passage control.

The FiRa (Fine Ranging) consortium is aiming to boost use of UWB technology, ensure UWB interoperability and grow the UWB ecosystem. In their words: ‘we’re committed to the widespread adoption of UWB-driven applications’ (https://www.firaconsortium.org). As an example, FiRa is developing Test Specifications for UWB PHY/MAC based on IEEE 802.15.4 standards. Activity related to UWB technology by big players like Bosch and Samsung in the FiRa consortium gives credibility to the technology.

2.1.4 Further research needs

More testing of VTT’s UWB system should be performed underground and near to big machines that reflect and block RF signals. Further studies and development of filtering and algorithms could be done to account for these different environments. The current VTT system does not support TAG to TAG communication. Determination of the proximity and location of nearby TAGs could be used for collision determination, for example with a machine-specific UWB network without fixed base stations, i.e. with BS’s located in moving machines.

Self-learning base stations position in fixed installations from only a few known survey points in the network’s relative coordinate system. This can considerably speed up deployment to new locations with fewer surveys and easier BS installation on uneven surfaces.

2.2 Wired Ethernet connectivity

Most of the current communication infrastructure underlying the existing IoT services provides best-effort quality of service at the data link layer. While many services, such as environmental sensing, can be built on such communication and the upper layers of the communication stack can provide guaranteed delivery of data and other quality-of-service characteristics, future IoT services are expected to include time-sensitive components such as real-time sensing and distributed control.

Currently available IoT services for mobile machines are primarily data collection only, with cloud connection provided with a cellular modem, WiFi connection or some other wide area networking technology. The emerging 5G network technologies, such as Ultra-reliable Low-Latency Communication and Multi-access Edge Computing, will provide the Quality-of-Service properties required for advanced real-time IoT services. Currently, mobile machine control is based almost exclusively on Control Area Network (CAN) technology, originally developed in the late 80s for the automotive industry. CAN provides multi-master serial bus communication protocol with bandwidth up to 1Mbps, although in practice 256 Kbps is often used. It has been observed at VTT and in industry that the low bandwidth of CAN has become an obstacle for developing advanced control applications and IoT services, and this will be even more so in the future when machines will be using advanced sensors, such as surround-view cameras, 3D scanners and radars, for (semi-)autonomous operation.

The automotive industry has already faced the same situation and has developed more advanced networking technologies for automotive networks. It is instructive therefore to look at the various technologies developed there and in other relevant industries. The sensors, actuators and Electronic Control Units (ECUs) of an automotive system communicate using an In-Vehicle Network (IVN). A modern automotive system typically has a hierarchy of networks, each with different properties connecting the ECUs (see Figure 4). A Local Interconnect Network (LIN) is a standardized (SAE JA2602), low-cost, serial communication (SCI, UART) network for low bandwidth applications such as switches, simple sensors and actuators. For higher bandwidth applications, CAN is the dominant network technology in the automotive sector. The protocol became an ISO standard in 1993. A more recent protocol CAN with Flexible Data-Rate (CAN-FD) can provide bandwidth up to 5 Mbps (specification was released in 2012). The limitations of even CAN-FD based technology have long since become apparent in automotive applications and, therefore, FlexRay technology is currently used in advanced automobile applications such as x-by-wire and Advanced Driver Assistant Systems (ADAS). FlexRay is an industry standard communication protocol providing a time-deterministic, redundant communication system providing bandwidth up to 10 Mbps. FlexRay is the state-of-the-art in the automotive industry and could be relatively easily adopted in the mobile machine industry as most microcontroller vendors providing chips currently used in CAN-based mobile machine control applications also provide comparable microcontrollers with FlexRay functionality.

Ethernet is the network technology of choice for office and telecom environments, and it is fast being adopted also in the automotive industry. The adoption of Ethernet technology is driven by economy of scale as it is the dominant networking technology, with huge investments in the development of fundamental technology, standards and special applications in multiple industries. The development and standardization of automotive Ethernet is on-going, with the Automotive Ethernet Congress and The IEEE-SA Ethernet & IP @ Automotive Technology Day being the premier venues for disseminating progress.

In vehicles, Ethernet is currently used in non-control applications such as diagnostics, firmware updates and entertainment systems. The latter area is standardized as Ethernet Audio Video Bridging (Ethernet AVB). The specific requirements of the automotive industry have motivated the

development of BroadR-Reach technology to serve as robust and cost-efficient Ethernet physical layer technology. BroadR-Reach technology provides bandwidth of 100 Mbps and beyond on a single twisted pair cable with reduced electromagnetic emissions. Ethernet is expected to become the high-bandwidth network backbone of vehicles as high data volume sensors such as surround-view cameras, 3D scanners and radars, and other systems supporting ADAS will overtax FlexRay.

Ethernet has one distinct disadvantage for use in control applications. The basic Ethernet does not guarantee any form of time-determinism. However, a number of extensions to the basic Ethernet exist that guarantee time-determinism and response times down to 1 ms. These derivatives of the Ethernet are often called the Industrial Ethernet and have been developed especially for process control in industrial environments. Perhaps the two best known technologies are EtherCAT and Profinet. The disadvantage of Industrial Ethernet technologies is that they are typically proprietary technologies driven by one or a few major companies and involve IPR licensing. However, since Industrial Ethernet technologies have been developed for use in harsh and hazardous environments, they have connector and cabling solutions for such environments including IP67/IP69K rated M8 and M12 connectors, oil and abrasion resistant, drag-chain compatible cables, and ruggedized IP67 switches. Some can also provide power over the standard cable and have special cables for high power supply.

While the automotive industry has taken a standards-based approach to adopting Ethernet, the aerospace industry has taken a proprietary technology development approach with Airbus developing and patenting Avionics Full-Duplex Switched Ethernet (AFDX) technology providing a time-deterministic, guaranteed quality of service network architecture based on commercial off-the-self Ethernet components. The technology is used in a number of airliners and is available for licensing.

In the agriculture and forestry field, ISOBUS is the standardized electrical interface between control systems on tractors and implementers. ISOBUS is based on CAN and thus also experiences its limitations. There has been research into replacing CAN with EtherCAT, and the Agricultural Industry Electronic Foundation managing the ISOBUS standard has a project team focusing on high-speed ISOBUS. It is highly likely they will adopt some form of Ethernet.
The advanced mobile machine control algorithms developed at VTT over the past few years and being shipped in the first products now have been implemented on existing commercial machine control systems. The limitations caused by computational power have been removed by the powerful multi-core microcontrollers that have become available during the development work. However, the 250 Kbps CAN bus used in the control system is a bottleneck and is expected to become more so in the next stages of development. In the short run, increasing the speed of the CAN bus or switching to FlexRay will remedy the current limitations. Nevertheless, in the foreseeable future, the high data volume sensors that will be used in driver assistance, remote operation, and automation will overtax FlexRay, necessitating the development of Ethernet-based control systems for mobile machines.

Deployment of one of the Industrial Ethernet technologies would be a straightforward solution, but avoiding licensing and vendor lock-in does not leave much choice in the technology selection. Only POWERLINK Industrial Ethernet is available as non-proprietary technology. It is implemented as a pure software stack on top of standard Ethernet (IEEE 802.3). It is free of patents and, furthermore, an Open Source reference implementation called openPOWERLINK is available under an extremely non-restrictive BSD license. Another attractive aspect of POWERLINK is that it includes CANopen mechanisms (object dictionary, PDOs, SDOs, etc.), making it conceptually easy to import applications developed for CANopen to POWERLINK. A disadvantage is that a special Ethernet MAC driver is required for hard real-time. openPOWERLINK provides a driver for a few select systems, but generally the driver must be developed or purchased for the intended target platform.

POWERLINK uses master-slave architecture in which the master node manages the slaves. In commercial embedded POWERLINK implementations, the master nodes are based on ARM A-series cores implying relatively high computational load from POWERLINK. In the TecNetwork project an attempt was made to revive an obsoleted POWERLINK slave implementation for a microcontroller based on ARM M-series core, but it was aborted due to incompatibility with the current Software Developing Kit.

Figure 5 presents a possible communication stack for a next generation mobile work machine enabling future real-time control and IoT services based on technology that is open and benefits from economy of scale. On the hardware side, it uses connectors and cabling from the Industrial Ethernet and the BroadR-Reach physical layer for robustness against electromagnetic interference and reduced electromagnetic emissions. Standard Ethernet higher layers would be used for broadband communication and hard real-time communication capability can be provided with POWERLINK either by porting the Open Source reference implementation to the computation platform in use or by acquiring or licensing a commercial implementation. For developing advanced distributed machine control algorithms, a scalable middleware framework supporting high-level software engineering concepts would be beneficial. Data Distribution Service (DDS) is one such standard framework developed by Object Management Group. Some commercial DDS implementations provide guaranteed communication latency enabling development of real-time control software at a high level of abstraction. Other communication protocols such as MQTT can connect to services at the Cloud and Edge Computing facilities. Some commercial Cloud Edge Computing service providers support device software development with full Software Development Kits, which have varying system requirements but minimally TCP/IP communication capability is required.

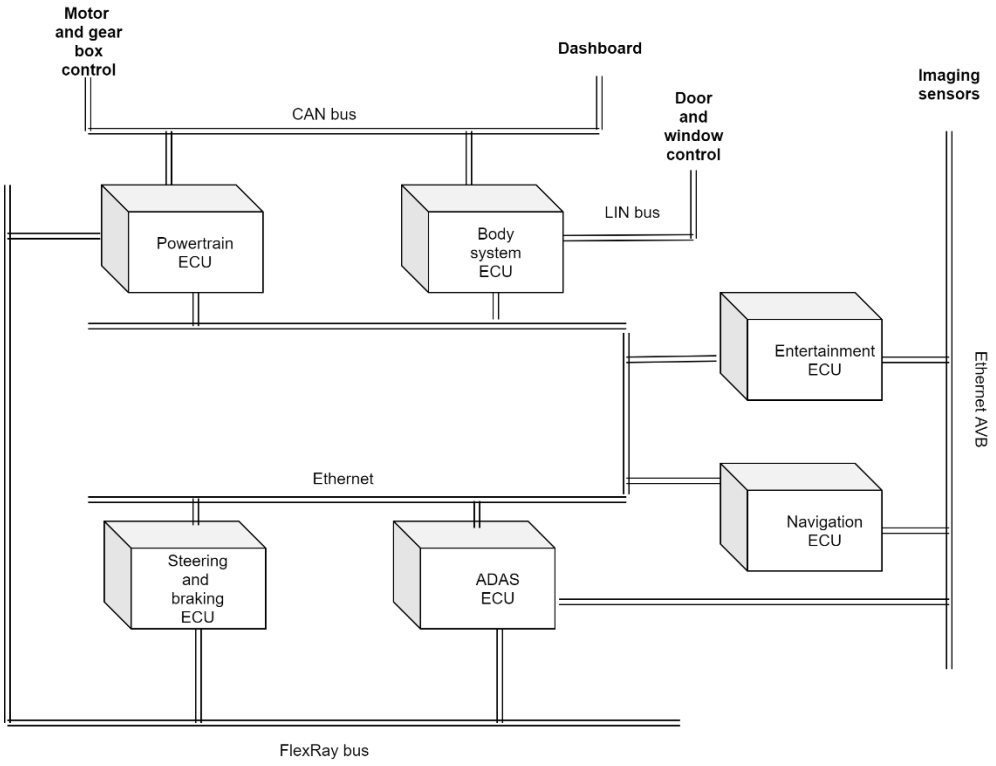


Figure 4. *A possible network architecture of an advanced vehicle.*

Small TCP/IP	DDS	Other	Device Profiles
			CANopen Application Layer
			POWERLINK Transport
			UDP/IP
			POWERLINK Driver
Ethernet Driver			
Ethernet MAC			
BroadR-Reach PHY			
EtherCAT / EtherCAT P M8 connectors & cables			

Figure 5. *A possible protocol stack for advanced mobile machine control enabling real-time control and IoT services.*

2.3 Cable-free power and communication

2.3.1 Introduction

Wireless instrumentation of sensors and actuators is becoming more and more common due to development of the IoT. Typically, wireless IoT devices are currently powered by primary (non-rechargeable) or secondary (rechargeable) batteries. In professional applications, using a battery may be inconvenient or a considerable cost factor over the lifecycle of the device, since the battery typically requires manual replacements or recharging even if the energy consumption of the IoT device is optimized. Wireless power transfer by means of RF far field as one solution to solve this has been proposed for many years, although it has not yet become common. With such a technical solution, wireless sensors and actuators could operate without batteries, which would otherwise eventually need maintenance.

Wireless power transfer could also replace power cables in applications where using cables is difficult or impossible, such as in the case of rotating machine parts that need to be monitored with wireless sensors. Avoiding cables and connectors can also save device installation costs, device encapsulation and galvanic isolation in the instrumentation of high-voltage objects, and cancel out the risks of cable and contact failures and galvanically coupled noise. An example of existing devices applying wireless power transfer with very limited capacity is passive (batteryless) RFID tags. RFID technology has also recently penetrated wireless sensor applications, although its powering capacity and wireless operation range are rather limited.

Cables and batteries for powering devices could also be replaced by energy harvesting from various sources of ambient energy, such as temperature gradients, vibration, light, and inherent RF fields. However, these are often very limited, case-specific and unpredictable energy sources in comparison to powering by an intentional wireless power transmitter.

2.3.2 System architecture

Figure 6 presents the overall architecture of wireless instrumentation with cable-free powering and communication investigated in the TecNetwork project. Figure 6 presents a generic architecture of

wireless nodes with power reception and bi-directional data transfer by UHF radio. Contrary to existing UHF RFID systems, the wireless nodes include an active radio transmitter to increase the wireless operation range. The wireless nodes also include interim energy storage to accumulate the received energy for future use, which also enables more advanced sensor and actuator features.

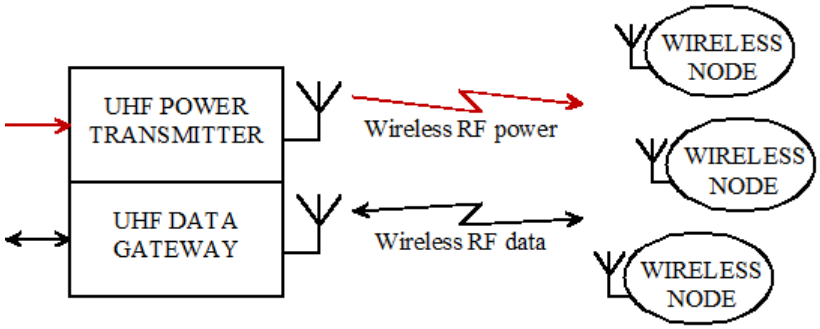


Figure 6. Generic architecture of the target system with cable-free powering and communication.

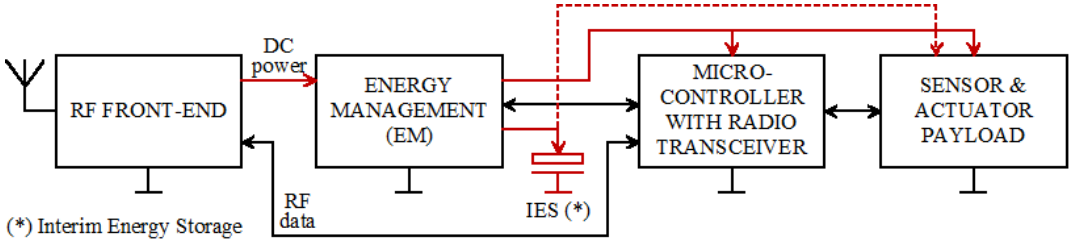


Figure 7. Generic architecture of wireless nodes with power reception and bi-directional data transfer by UHF radio. Powering paths are indicated in red.

For the wireless operation range and powering capacity, the most critical part of the wireless node is the RF front-end that has to take care of generating relevant DC power from the received RF power with maximal performance and connecting the bi-directional RF data signal to the antenna with minimal losses. Several technology options for the RF front-end, either with one shared antenna or two separate antennae for powering and communication, were investigated, simulated and prototyped.

2.3.3 Pilot system

For practical performance evaluations, an integrated pilot system, consisting of a macroprototype wireless node (Figure 8), 2.45 GHz UHF magnetron based 500 W power transmitter (Figure 9) and a UHF data gateway connected to a PC, was implemented and tested.

The macroprototype wireless node was based on a VTT proprietary wireless communication node (Little Node, developed in earlier projects) for realization of the microcontroller, radio transceiver and temperature sensor payload (see Figure 7). The macroprototype wireless node also included a commercial Texas Instruments bq25570 evaluation kit for energy management, and a customized printed circuit board (PCB) for the antennae, RF front-end and interim energy storage. The PCB included several antenna and RF front-end options for practical evaluation.

Performance tests of the integrated pilot system were conducted outdoors by applying separate antennae for powering and communication. The communication branch used the in-built antenna of the Little Node and the power reception branch consisted of either a sleeve dipole or a commercial monopole antenna connected to an SMA connector in the customized PCB. Energy storage was provided by a 220 mF supercapacitor, 4700 μF electrolytic capacitor and a 100 μF ceramic capacitor connected in parallel. The wireless operation distance was 10 m.

Power transfer performance was measured by measuring the charging time of the energy storage from empty (0 V) to full (5.3 V), which was around 25 minutes. This gives a mean charging power of 2.1 mW. The total received power level is slightly higher due to the losses of the energy management electronics, sleep-mode current consumption of the Little Node, and the leakage current of the energy storage.

The total energy consumption from the energy storage per one activity cycle carried out by the Little Node for temperature measurement and associated communication with the UHF data gateway was also measured. The result was 17.4 μJ. This is less than 1% of the accumulated energy during a 1-second power transfer period. Thus, much more energy consuming sensor applications with even lower power transfer levels would be possible even if the measurement rate would be once a second.

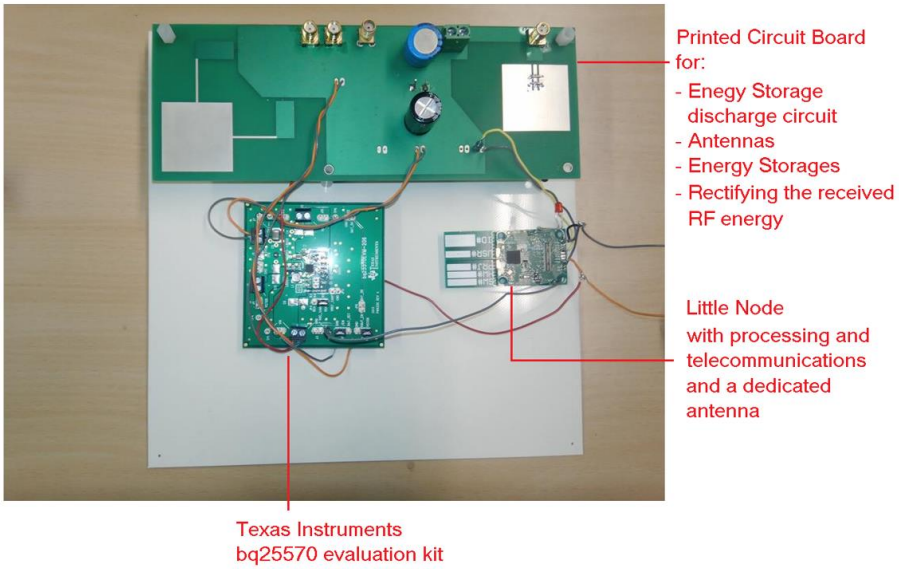


Figure 8. Macroprototype wireless node of the pilot system.

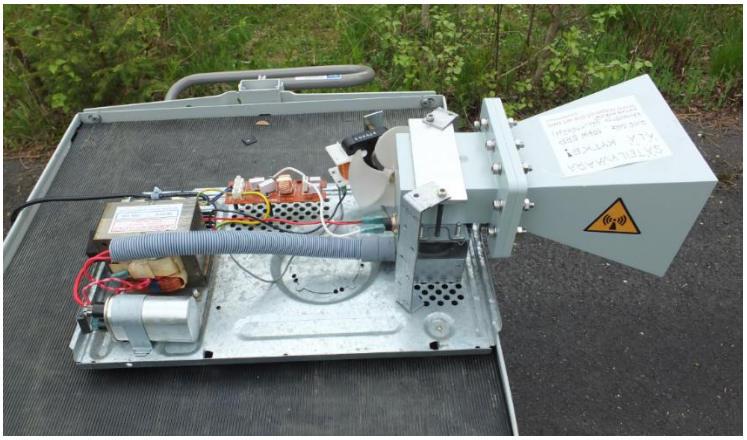


Figure 9. UHF power transmitter of the pilot system.

2.3.4 Safety and regulatory issues

In the EU, occupational RF exposure is regulated by directive 2013/35/EU and further in Finland by government act 388/2016 and Ministry of Social Affairs and Health act 294/2002. The latter concerns the exposure of the public only. The exposure limits in these documents derive from the International Commission on Non-Ionizing Radiation Protection (ICNIRP) Guidelines 1998.

Directive 2013/35/EU gives two procedures for showing compliance with the exposure regulations. In the simplified procedure, all that is required is to show by measurements or calculations/simulations that the electromagnetic field strength is below the action limits in the workplace with workers not present. For example, the action limit for the electric field at 2.4 GHz is 140 V_{RMS}/m. In plane wave approximation, this corresponds to a power density of 52 W/m^2. The power transmitter of the pilot system has a 500 W magnetron and a horn antenna with 15 dBi gain. By applying these design parameters in free space, the calculated power density limit is intercepted at a distance of 4.92 m.

The action limits are chosen to be very conservative. They produce an exposure situation in which the specific absorption rates (SAR) [W/kg] in all body parts remain well below the limits even in worst-case scenarios. The second procedure is for situations where the action limits are exceeded but the actual SAR values can still be shown to comply with the limits. This requires actual measurement or careful simulation of the SAR values on exposed body parts. This can be a very complex and expensive undertaking. The employer is required to have a plan in place to prevent exposure where the SAR limits can be exceeded. In addition, other measures may be required by legislation.

The applicable EMI/EMC standard for the communications branch is ETSI EN 300 440 (Short range devices; Radio equipment to be used in the 1 GHz to 40 GHz frequency range). The power transmission branch does not support data communications, so the regulations for Industrial, scientific and medical (ISM) systems apply. Spurious emission limits for the ISM systems are put forward in the CISPR (Comité International Spécial des Perturbations Radioélectriques) standard CISPR11:2015. Licensing policy for 2.4GHz power transmission using high power may vary from country to country. Discussions with the Finnish Communications Regulatory Authority pointed out that even if the license is required, it is much more easily granted for an ISM band application. In the mine environment, general guidelines for EMI/EMC issues concerning explosives in MIL-STD-464C may also be relevant.

2.3.5 Summary and conclusions

The technical feasibility of batteryless wireless nodes by applying wireless powering and communication by UHF radio has been studied. The study also included a pilot system, operating by interleaved long powering periods and short activity cycles with message exchange between the wireless node and a data gateway by an active radio transmitter at both ends.
The theoretical evaluations and the measurements by prototypes of separate building blocks and an integrated pilot system indicated that the target system concept is feasible. Depending on the required wireless distance, energy consumption of the activity cycles of the wireless node, and the interval between the activity cycles, power transmission levels that require specific considerations of human safety and compatibility with the EMI/EMC regulations may however be needed.
The TecNetwork project resulted in a new technology platform for batteryless wireless sensor nodes with wireless UHF-band (2.4 GHz) powering and communication. The focus of follow-on activities should be targeted at its applications, which should be addressed case-by-case. The follow-on activities should also involve benchmarking performance against novel existing commercial solutions, such as those of Powercast.

Detailed results are presented in a separate report[1].

[1] Strömmer, E. Tanskanen, A. & Ylisaukko-oja, A. 2019. Energy Autonomous Wireless Sensors and Actuators with Powering and Communication by UHF Radio. Available at: https://www.vtt.fi/sites/tecnetwork/PublishingImages/results/VTT-R-00472-19_Public.pdf

3. Control system development towards autonomous machines and processes

The demand for automated and remotely operated machines arises from the need to improve the safety, quality, cost-efficiency and traceability of work processes. Ecological issues and sustainable development require minimizing resource losses while maintaining or even improving quality standards. The road map introduced in section 3.1 offers a long-term perspective on the technological evolution as machine builders introduce new automation features over time to respond to the needs of customers. The aim of the road map is to help machine manufacturers and technology providers identify their current technological readiness and to guide their way towards autonomously operating remote machines. In section 3.2 the enabling technologies for autonomous operation are discussed in more detail.

3.1 Roadmap towards autonomous mobile machines

The roadmap towards autonomous machines starts from manually operated machines (Figure 10). Manual operation in this context means that the human operator controls the actuators of the machine in a feed-forward fashion (Figure 11). Based on this definition, both early 1900s cable driven booms and modern booms with electro-hydraulic actuators belong to the same manually operated machine category. The schematic control architecture of a manually controlled machine shown in Figure 11 implies that the operator directly controls separate actuators with multiple control devices, which may be physical or digital.

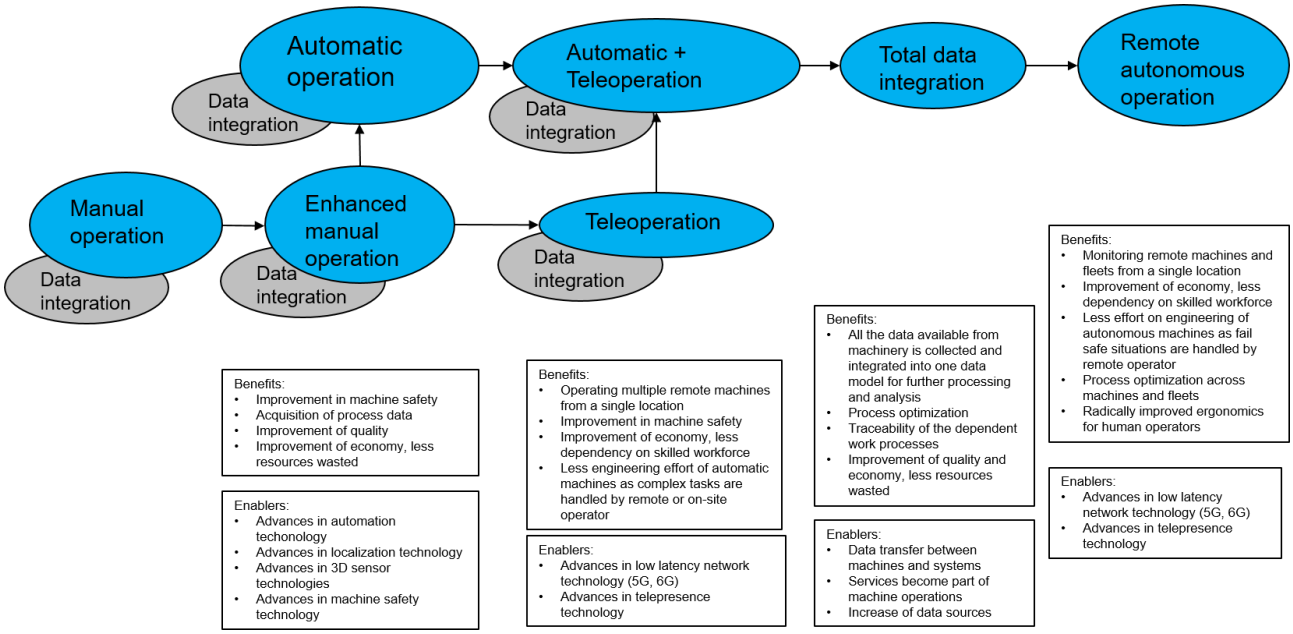


Figure 10. *Roadmap towards autonomous mobile machines*.

Data integration of the manually operated machines typically involves acquisition of work process data for assisting the operator to achieve higher quality with less resource waste. Examples of existing data integration systems available for manually operated machines are Normet SmartScan[2] for concrete spraying machines and Novatron Xsite[3] software products for loaders, dozers, surface drills and piling rigs[4].

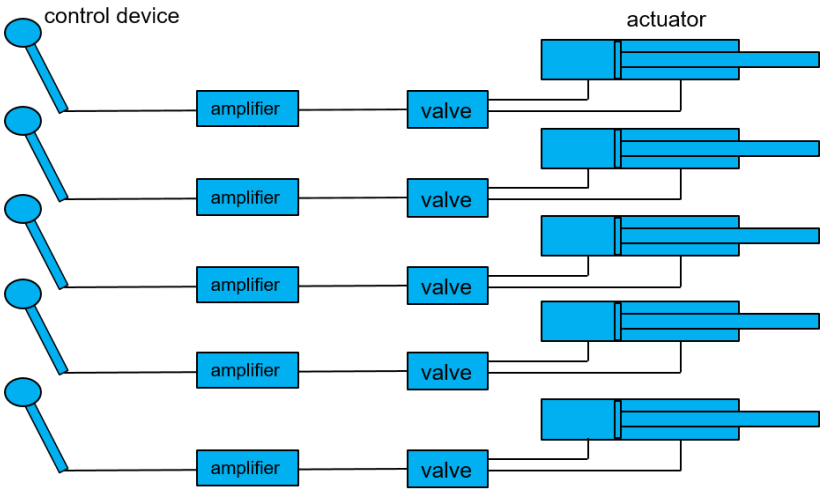


Figure 11. *Schematic control architecture of a manually operated machine*.

As the level of automation of manually operated machines increases, the next development phase is typically a machine with enhanced manual operation. Enhanced manual operation requires the operator on site to control the machine, but not necessary each actuator separately. Good examples of machines with enhanced manual operation are Cartesian control of the excavator bucket or of the nozzle of the concrete spraying boom, such as in Normet SmartSpray Lite[5]. Novatron Oy offers the RTEC™ automation system to upgrade existing manually operated excavators with automation features such as controlling boom movement and speed and preventing flipping and overloading of the machine.

The schematic control system architecture of an enhanced manually operated machine is shown in Figure 12. In the exemplary architecture, the human operator controls a group of actuators with a single control device. The manual motion controller, for example running kinematics computations, produces the reference control signals for the separate actuators. The position controller produces control signals for the actuators based on the reference positions and the measured positions of the actuators. Actuators with position, velocity or force feedback, commonly called servo actuators, are fundamental components of robotic systems and are prerequisites for the development of more advanced automatic features of mobile work machines.

[2] Normet Group Oy. 2019a. Normet SmartScan. https://www.normet.com/smartscan/. Accessed 21.5.2019.
[3] Novatron Oy. 2019a. Machine Control Systems. https://novatron.fi/en/systems/ Accessed 21.5.2019.
[4] Novatron Oy. 2019b. Automation for excavators. https://novatron.fi/en/automation-for-excavators/ Accessed 21.5.2019.
[5] Normet Group Oy. 2019b. Normet SmartSpray. https://www.normet.com/smartspray/. 21.5.2019.

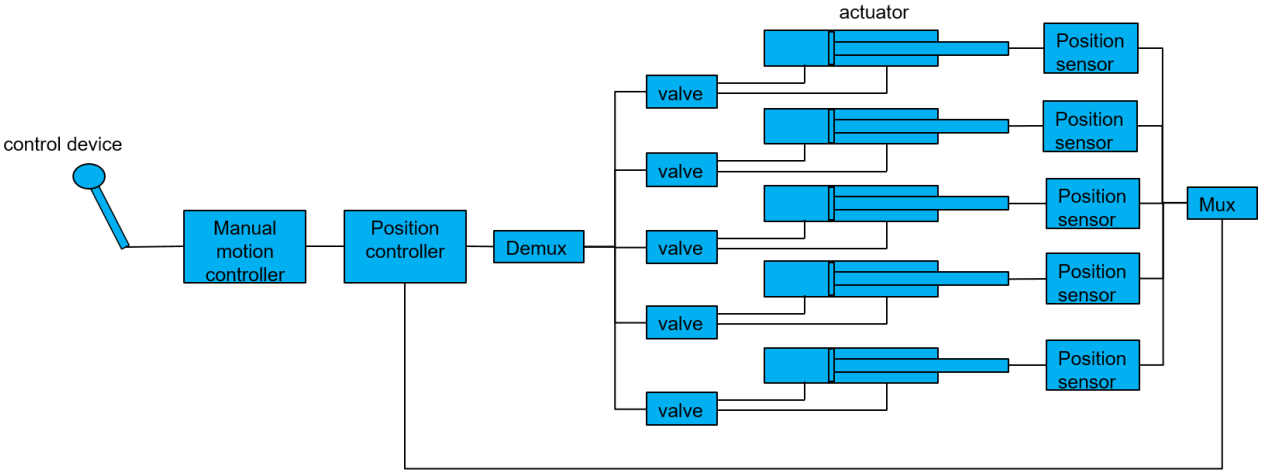


Figure 12. *Schematic control architecture of a machine with enhanced manual operation*.

The next step up from enhanced manual operation is to develop automatic features or to extend the machine with a teleoperation interface. The chronological order of introducing automatic and teleoperation features depends on the machine type, business environment and machine builders' strategic choices. In some cases, automation and teleoperation are developed concurrently resulting in the machine including both automatic and teleoperation features. Teleoperation is needed, as it is hard to develop robust automation for complex tasks in real-world working environments, and teleoperation enables combining the intelligence and flexibility of the human operator with automated machines regardless of their location.

In the mining industry, teleoperation of machines improves ergonomics and safety, as operators do not need to enter or stay for long periods in hazardous areas. Existing teleoperation systems utilize the machine vendor's proprietary communication channels and network infrastructure, which need to be built and maintained by the machine vendor or end-user. In the near future as commercial low latency 5G wireless networks will be launched, it is expected that networks enabling teleoperation will be available as a service.

The schematic architecture for a machine with automatic operation mode is shown in Figure 13. In this case, the operator on site can control the machine in enhanced manual operation mode or switch the machine to automatic operation mode. When the machine is in automatic operation mode, the operator constantly monitors the machine and is able to switch back to manual operation mode as necessary. It is assumed that the operator handles fault situations manually, as early automatic features typically cannot handle more complex work tasks.

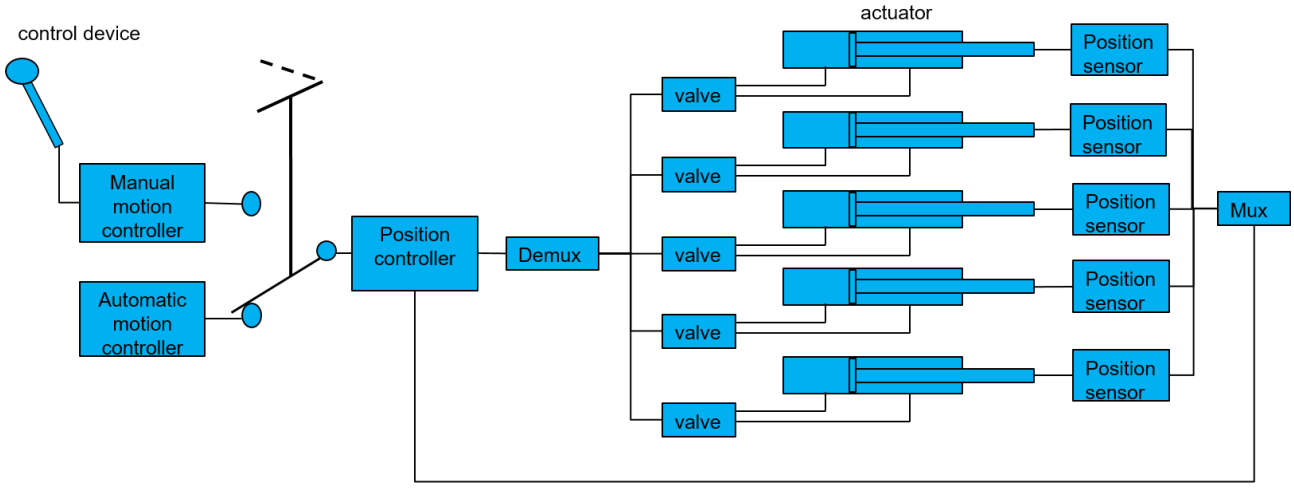


Figure 13. *Schematic architecture of a machine with automatic operation mode*.

When the automatic machine is extended with a teleoperation interface, the remote operator can connect to the machine via a low latency network and monitor the machine via a real-time video stream (Figure 14). The remote operator is able to control the machine manually or optionally switch the machine to automatic operation mode.

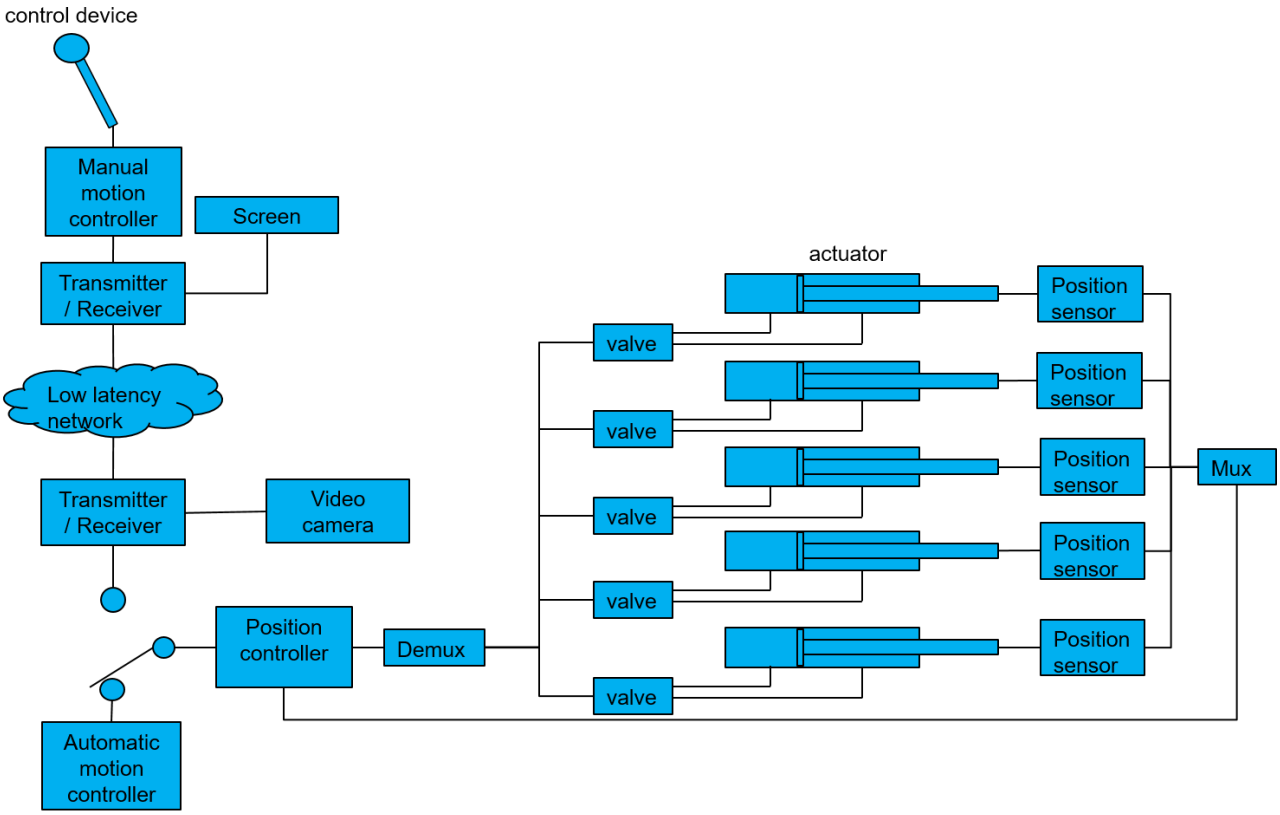


Figure 14. *Example schematic control architecture for a teleoperated machine with automatic operation mode*.

Machines with automatic or teleoperation features, or both, currently exist. For example, Normet provides the software packages SmartSpray Pro and SmartSpray ProPlus for concrete spraying booms enabling automatic movement primitives. Sandvik's Automine product line[6] combines autonomous navigation of loaders with teleoperated loading and dumping[6]. In Sandvik's Automine concept, the teleoperator monitors and controls the automated machines from a safe remote control room.

Data from various sources is integrated in all phases of the roadmap, enabling traceability and optimization of the work process as well as communication between machines. The level of automation affects the content of the integrated data. In the manually operated machines, the data is typically used for optimizing the work process and guiding the operator in achieving higher quality and reducing resource losses. The automated and teleoperated machines provide both work process data and detailed machine control data related to navigation, actuators and vehicle statuses. In addition, teleoperated machines provide video and audio streams from the machine to the remote control room.

Total data integration is a prerequisite for remote autonomous mobile machines. In total data integration, all available data from the machinery is collected and integrated into a single data model for further processing and analysis. The integrated data model forms a basis for process optimization using data analysis and machine learning. The remote autonomous operation means radically improved ergonomics, as the human operators are removed from difficult and hazardous environments into office-like control rooms.

The final development phase of the roadmap is remote autonomously operating machines that are connected via a low latency network (Figure 15). In the future, autonomous machines will be capable of accomplishing more complex tasks than their automatic predecessors. Due to robust automation, remote autonomous machines are capable of operating long periods without direct user intervention. However, remote autonomous machines also include a fail-safe mode in case of unexpected breakdowns, which can be conveniently handled by the remote operator via a teleoperation system.

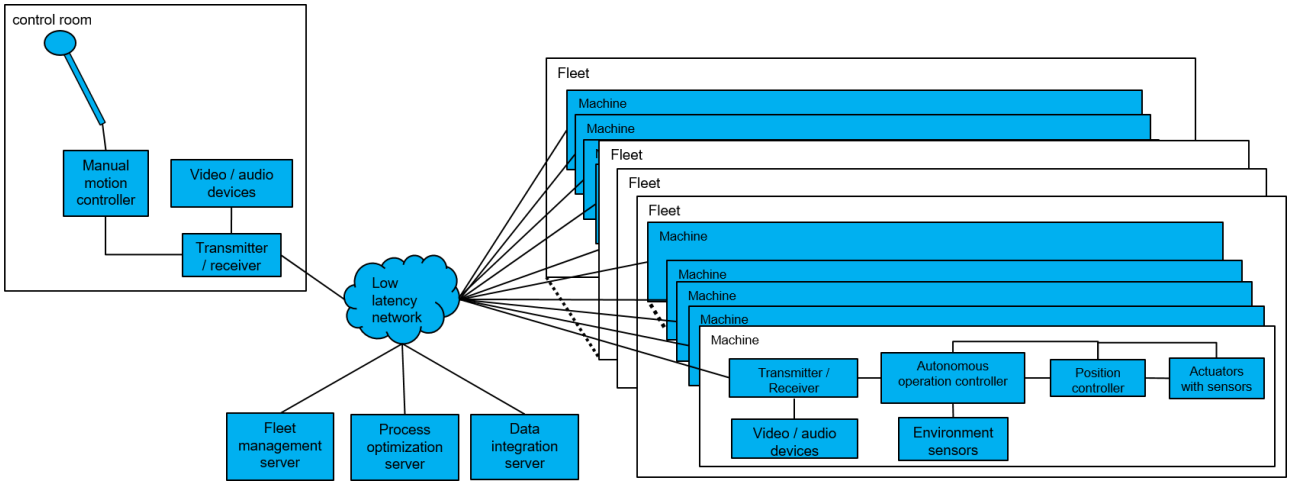


Figure 15. *Schematic control architecture of remote autonomous machines and fleets*.

[6] Sandvik AB. 2019. Automine Equipment Automation and Teleoperation Systems. https://www.rocktechnology.sandvik/en/products/automation/automine-equipment-and-teleoperation-systems/. 21.5.2019.

3.2 Development of computer-assisted control and autonomic features

As mobile work machines are typically used in varying environments, automatic or autonomous machines need to be able to sense and adapt to changes in the environment. Thus, the most fundamental control features required are 3D perception and collision-free path planning. Both areas have been investigated for decades, and work machine builders may significantly benefit by adopting existing methods and algorithms. Section 3.2.1 provides a review of previous research and path planning problem formulation, and Section 3.2.2 introduces an open-source state-of-the-art and most widely used software package for collision-free path planning named ROS MoveIt.

3.2.1 Planning of collision-free paths

Planning collision-free motions and paths is a fundamental property of an autonomous machine. Path planning has been a well-researched subject over the years, and the work has resulted in a large collection of available planning algorithms. The algorithms can be divided to two main approaches: sensor-based and model-based algorithms. Sensor-based algorithms compute the paths directly from the sensor output without creating an environmental model. They can be very fast on inexpensive computation platforms such as microcontrollers, enabling low-cost real-time control systems. Due to their simplicity and local nature, they cannot produce optimal solutions and can fail often in complex environments. Sensor-based algorithms are often reactive, meaning that they plan just a single action at a rate determined by the rate that the used sensor produces data. Reactive planners are inherently applicable in dynamic environments. As an example, early robotic vacuum cleaners used reactive path planning.

Model-based path planning algorithms assume a complete model of the environment as an input. Classically, model-based path planning algorithms were developed in the field of computational geometry in order to solve what is called a Piano Mover's Problem: to compute a collision-free path for a rigid movable object among obstacles from one position to another. This early theoretical research produced a number of results describing the computational complexity of various formulations of the path planning problem[7]. It is currently understood that the path planning problem is PSPACE-hard, i.e., the algorithm's space requirement grows exponentially with the size of the problem. In particular, it grows exponentially in the number of parameters required to completely specify the position of every point of the movable object. That number is called the number of degrees of freedom of the movable object. This result means that the path planning problem is intractable, and for every algorithm it is possible to present problem instances that the algorithm fails to solve with any given finite computational resources.

In parallel to theoretical research, many algorithms were developed and presented to be used in solving actual path planning problems arising in robotics. Perhaps the most important of these was the Randomized Path Planner (RPP) introduced in 1990, as it demonstrated that many interesting path planning problems with more than six degrees of freedom could be solved in practical time[8]. RPP constructed a potential field in the environment by combining attractive potential towards the goal position and repulsive potential towards obstacles. Gradient descent was used to search a

[7] Sharir M., Algorithmic Motion Planning, In Goodman J.E., O'Rourke J. (eds), Handbook of Discrete and Computational Geometry, CRC Press, Boca Raton, Florida, 1997, 733-754.
[8] Barraquand J., Latombe J.C. A Monte-Carlo Algorithm for Path Planning with Many Degrees of Freedom, Proceedings of the 1990 IEEE International Conference on Robotics and Automation, IEEE, 1990, 1712-1717.

path towards the goal backed by random walks to escape local minima. RPP was a purely kinematic path planner, i.e. it did not assign time to the path to create a trajectory. Smoothing out the random walk sections and assigning time to the smoothed path in a post-processing stage was required for computing trajectories executable by a physical robot.

Kinodynamic planners plan simultaneously for position and velocity and can produce trajectories directly executable by a physical robot. One of the notable kinodynamic planners is the Rapidly-Exploring Random Tree (RRT)[9]. Many variants of RRT and similar randomized algorithms have since been presented in the scientific literature.

While randomized path planners exhibit good empirical performance, due to their randomized nature they often produce paths that are suboptimal in some desirable metric and it can be difficult to incorporate constraints on the resulting trajectory. Optimal path planners that optimize a particular metric, such as time or energy consumption, and constrained path planners that compute paths or trajectories fulfilling a particular constraint, such as keeping the tool control point on a given Cartesian curve, often use different approaches. When creating constraints for the trajectories, the constraints must be definable mathematically to be included in the problem formulation.

For planning in dynamic environments, model-based path planning algorithms can be used in a re-planning loop where the environmental model is periodically updated with new sensor data and the path is planned again or the previously computed path is modified after each sensor data update. On modern computing platforms, randomized path planning algorithms are often fast enough to operate in near real-time, so the re-planning does not significantly slow the robot operation.

It should be pointed out that the above presentation relates primarily to autonomous machine process control, such as planning motions for a robot manipulator or a boom. In such a case, the environmental model is created for fast collision detection and possibly for calculating the minimum distance to the obstacles. Fast collision detection or minimum distance calculations are challenging research problems on their own and fall beyond the scope of this report, other than pointing out that efficient implementations are available as open source software. Planning paths for the mobility of the autonomous machine is a related but distinct problem where the environmental model becomes the focus of the research and development. Creating terrain and obstacle models and suitable path planning algorithms for autonomous driving are also beyond the scope of this report.
For a more detailed overview of the computational complexity of path planning and randomized path planning algorithms up to 2003, see chapter 4 in Isto 2003[10]. For a more recent survey including classifications and assessments of various path planning approaches with references to original research papers, see Yang et al. 2016 [11].

To summarize, planning a collision-free path between two points requires a robot model, an environmental model and a collision-detection algorithm in addition to the actual path planning algorithm. The environmental model can be achieved with 3D depth sensors providing a 3D image of the robot's surroundings and combining multiple images as a complete model. Dynamic environments require updating the model iteratively and re-planning or modifying of the previous plan. The planned path must be communicated to the robot controller and executed in it, possibly with option of dynamic re-planning. Robot simulation and visualization are essential during system

[9] LaValle S.M., Kuffner J.J, Randomized Kinodynamic Planning, Proceedings of the 1999 IEEE International Conference on Robotics and Automation, IEEE, 1999, 473-479.
[10] Isto P., Adaptive probabilistic roadmap construction with multi-heuristic local planning, Doctoral Dissertation, Helsinki University of Technology, 2003.
[11] Yang L., Qi J, Song D., Xiao J., Han J, Xia Y., Survey of Robot 3D Path Planning Algorithms, Journal of Control Science and Engineering, Volume 2016, Article ID 7426913

development. Integrating all of these components and a robot into one system is a substantial engineering task.

3.2.2 ROS MoveIt motion planning framework

The open-source software package ROS MoveIt[12] has all of the previously mentioned components integrated and much more. The Robot Operating System (ROS) is an open-source, meta-operating system for robots[13]. It provides a common framework full of services for robotics applications including hardware abstraction, low-level device control, message-passing between processes and so on. The MoveIt software runs on top of ROS and provides functionality for kinematics, motion/path planning, collision checking and 3D perception, as well as a host of other functions. MoveIt is currently supported only in Ubuntu (Linux), but a Windows 10 version is being developed. Our experiments were performed with Ubuntu version 18.04 and the Melodic version of MoveIt.

The main advantage of MoveIt is its huge collection of ready-to-use features. It provides a visualizer for the simulations, collision checking, multiple solvers for inverse kinematics, motion-planning algorithms, and a setup assistant for creating a virtual robot model for a custom robot or deploying the over 100 robot models provided by the community. All of which can be taken into use as needed.

The MoveIt visualizer is based on the ROS 3D Visualization tool (RViz) shown in Figure 16. In addition to the default functionalities, such as adding point cloud sources and coordinate frames, MoveIt's RViz has customized menus for configuring path planning algorithms and adding scene objects.

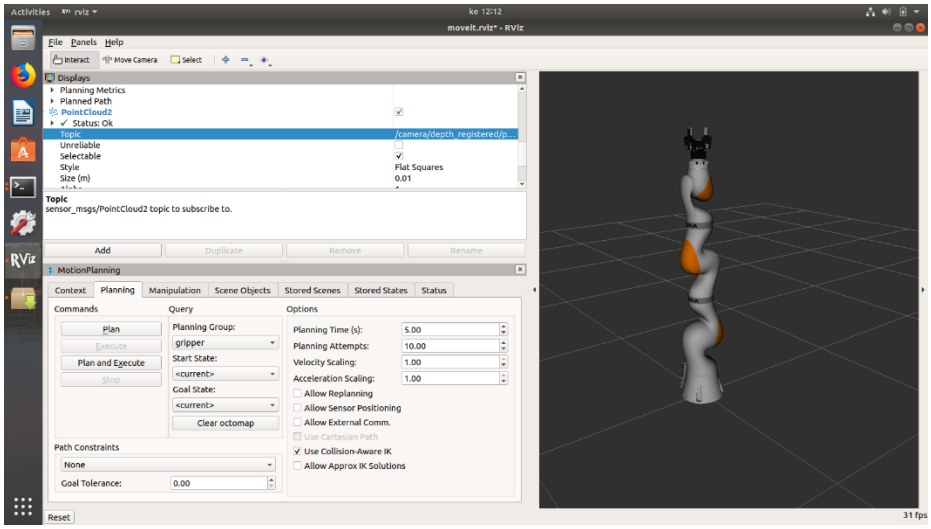


Figure 16. *Image from the simulation environment*.

All of MoveIt's motion-planning algorithms come from the Open Motion Planning Library (OMPL)[14]. OMPL is a library, which itself does not contain any code related to collision checking or visualization; it only holds a group of motion planning algorithms, any of which can be easily implemented. It contains implementations of sampling-based algorithms such as PRM, RRT, EST, SBL, KPIECE, SyCLOP and other variants of these planners. All of these planners work only in joint space, which means that Cartesian paths cannot be planned with OMPL algorithms. The

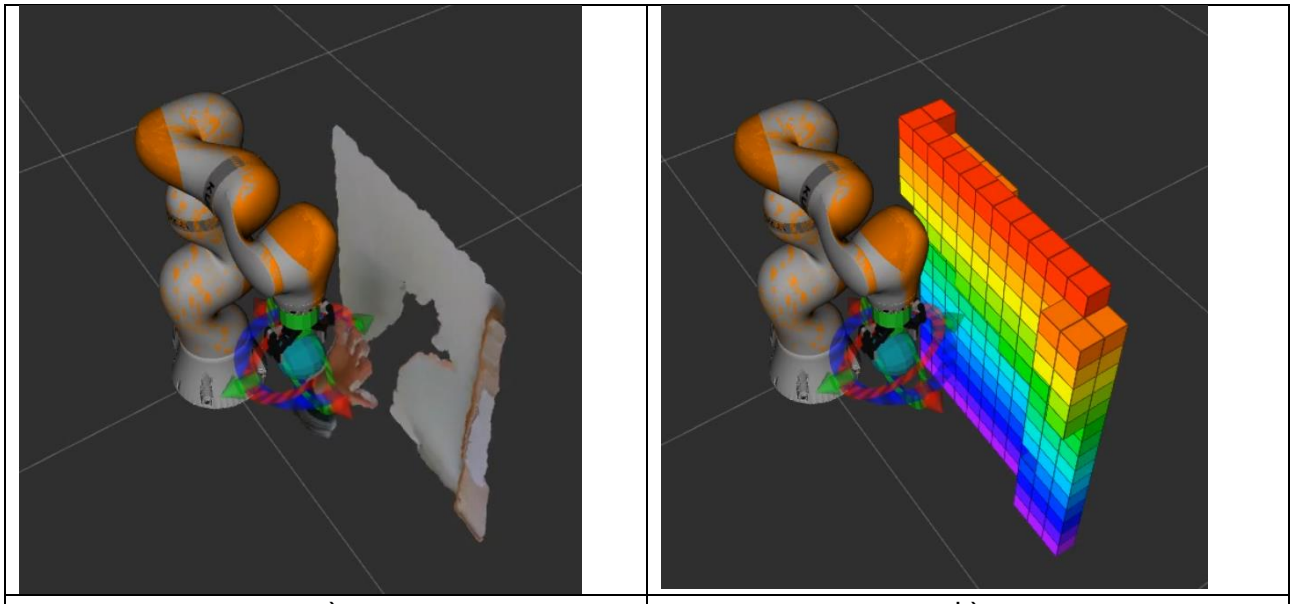
[12] MoveIt. https://moveit.ros.org/]. 13.8.2019.
[13] Robot Operating System (ROS) Wiki, 2019. http://wiki.ros.org/ROS/Introduction. 13.8.2019
[14] The Open Motion Planning Library (OMPL). https://ompl.kavrakilab.org/. Accessed 13.8.2019.

planner will only solve the free path between two joint-positions, which can then be executed in a simulation or with a real robot using MoveIt.

Whereas OMPL works only in the joint space, algorithms have been developed for Cartesian path planning. In MoveIt, such an algorithm is called Descartes[15]. Descartes is a part of the ROS-Industrial project, which is a part of ROS that extends the advanced capabilities to manufacturing automation and robotics. With Descartes, semi-constrained Cartesian paths can be planned. Semi-constrained path means that some waypoints may be 'Axial symmetric', in which the tool can be freely positioned relative to a given axis. This is very practical in common applications such as welding and painting, where the perpendicular orientation of the tool relative to the surface does not affect the outcome. We tested the Descartes algorithm, but found it to be quite experimental at best. It is also computationally much more challenging than joint-space path planning, since the Cartesian path first needs to be transformed to joint space. Moreover, finding all possible solutions in joint space is quite demanding for an inverse kinematics solver. There are some solvers available, but most are restricted to a maximum of 7 degrees of freedom, which restricts their use in custom robots.

Although MoveIt includes a collection of the most common robots from multiple manufacturers, it also provides a way to create custom virtual robot models. The requirements for the custom robot model are 3D models of the parts in STL format (for each joint and link) and Denavit-Hartenberg (D-H) parameters, which describe the distance and the angle between the two consecutive links. With the 3D models and D-H parameters, Unified Robot Description Format (URDF) can be created.

Because ROS is a commonly used framework for 3D perception systems, it is relatively easy to integrate 3D sensors into MoveIt. This allows the addition of a sensor to the robot system that uses a measured 3D point cloud to create an occupancy grid in the workspace. The path planner considers the occupancy grid as an obstacle and avoids collisions with it. Figure 17a shows an example where the point cloud measured with Intel's RealSense D415 depth camera was streamed to the ROS MoveIt. Figure 17b shows the occupancy grid computed based on the measured point cloud.



a) b)

[15] The ROS Descartes package summary. http://wiki.ros.org/descartes. Accessed 13.8.2019.

Figure 17. *a) The point cloud measured with Intel Realsense D415 visualized in the ROS MoveIt simulator and 2. b) the obstacle visualized as an occupancy grid*.

MoveIt is highly modifiable to different situations depending on the process and requirements. Its main downsides are that it is only partially tested open-source software and it has specific Linux packet dependencies. In addition, being open-source software means that there is no backing organization to guarantee bug fixes or provide updates. On the other hand, MoveIt provides numerous integrated components that would otherwise require considerable development and programming work. MoveIt thus enables very fast implementation of proof-of-concept demonstrations and early 0-series prototypes. In addition, due to the BCD license [https://opensource.org/licenses/BSD-3-Clause], everything non-essential can be stripped from MoveIt and the essential code used with other custom software. Commercialization of MoveIt's functionalities would require establishing a private version control repository of MoveIt's source codes and readiness to maintain the commercial source codes for the whole life cycle of the product.

3.2.3 Boom deflection modelling with neural networks

We tested the usability of neural networks for modelling deflections with Keras on top of TensorFlow libraries. Keras is a front-end open source neural network library that can be used on top of TensorFlow, Microsoft Cognitive Toolkit, Theano, or PlaidML.

The training data and testing data were all acquired from a simulator, so the results are not usable in a real-world environment. For the data acquisition we developed an external software for controlling the positions of the joints, so that the same data acquisition runs could be run multiple times.

The tested neural networks had five inputs: Boom1_Lift, Boom1_Zoom1, Boom1_Zoom2, Boom2_Zoom1 and Boom2_Zoom2, and two outputs: SprayingHead_x and SprayingHead_y, that designate the position of the spraying head motor in the x-y plane. The x coordinate describes the distance from the base, and the y coordinate the distance from the floor, so the deflections are shown in the y coordinate value. The input values were normalized before training and testing.

The neural network structure was varied in an attempt to find the best working structure. The number of hidden layers was varied between 2 and 6, and the number of nodes per hidden layer was varied between 8 and 64. The hidden layers were pairs of ReLU and linear layers, so that the first tested neural network had one pair of ReLU and linear layers, the second network two pairs, and the last three pairs.

The networks used the mean squared error loss function and the Adam optimizer.

Training and testing with data acquired from a single simulator run

The following figures show the training and testing data acquired from a single test run in the simulator. The first half of the acquired data was used in training, and the rest in testing.

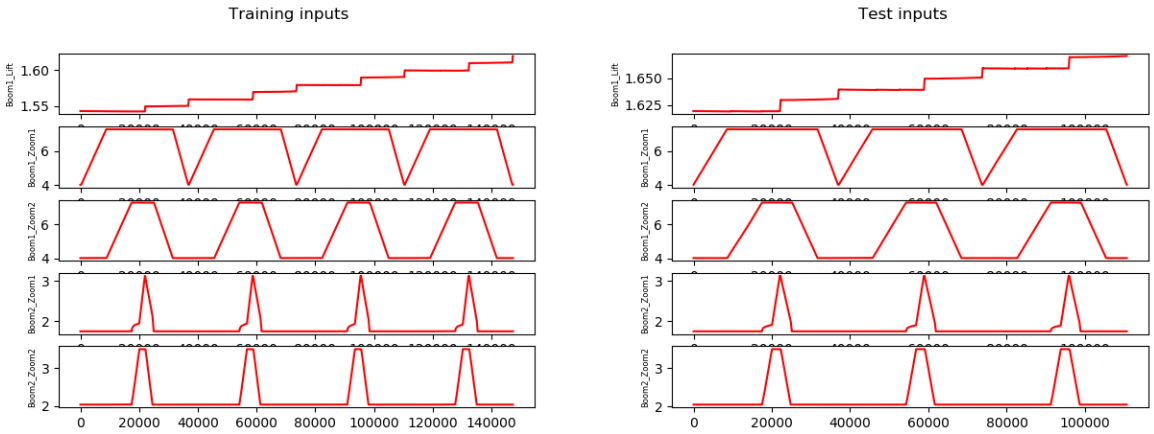


Figure 18. Unnormalized training and testing inputs.

The following figures show the training and testing results with different neural network structures. In the figures, the red graphs represent the values received from the simulator, and the blue graphs the values given by the neural network.

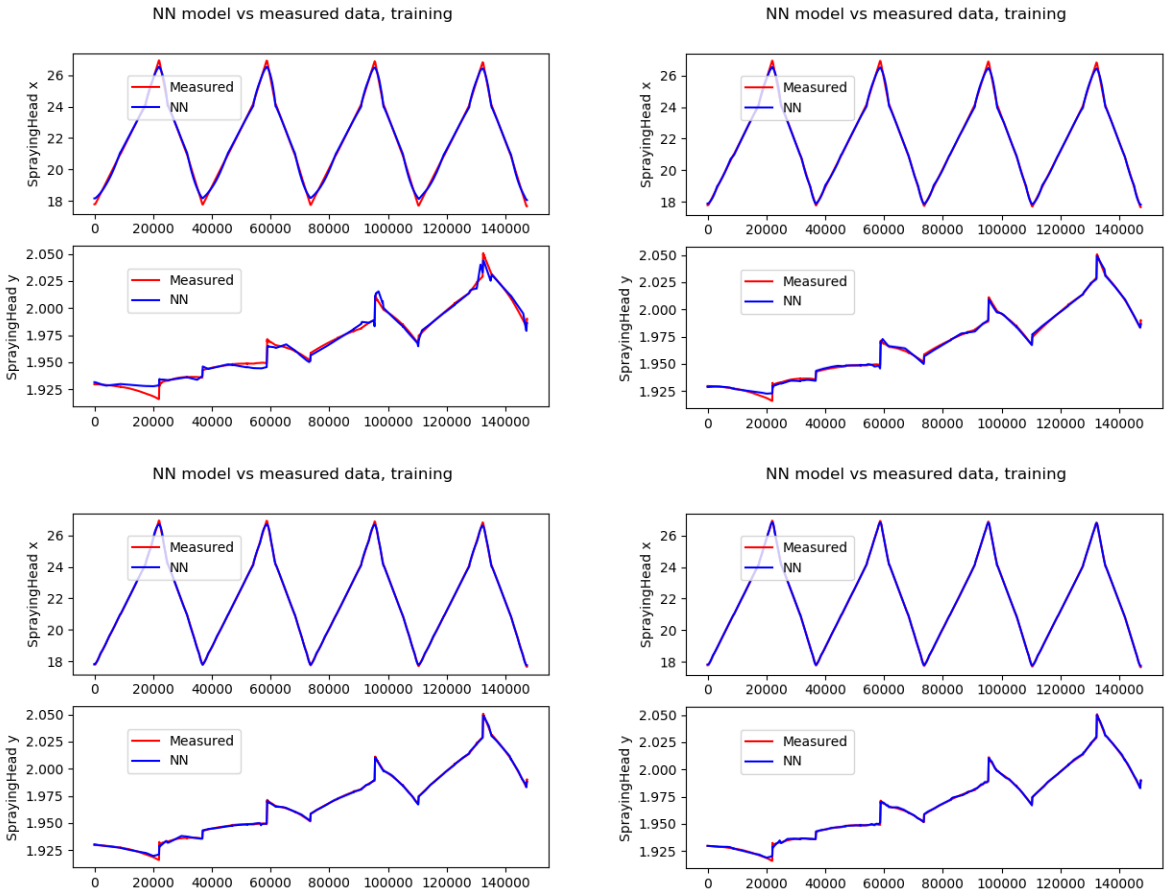


Figure 19. Training results for a neural network with 2 hidden layers with a varying number of nodes per layer. The first figure, top left, has 8 nodes per layer, top right has 16 nodes per layer, bottom left has 32 nodes per layer, and bottom right 64 nodes per layer.

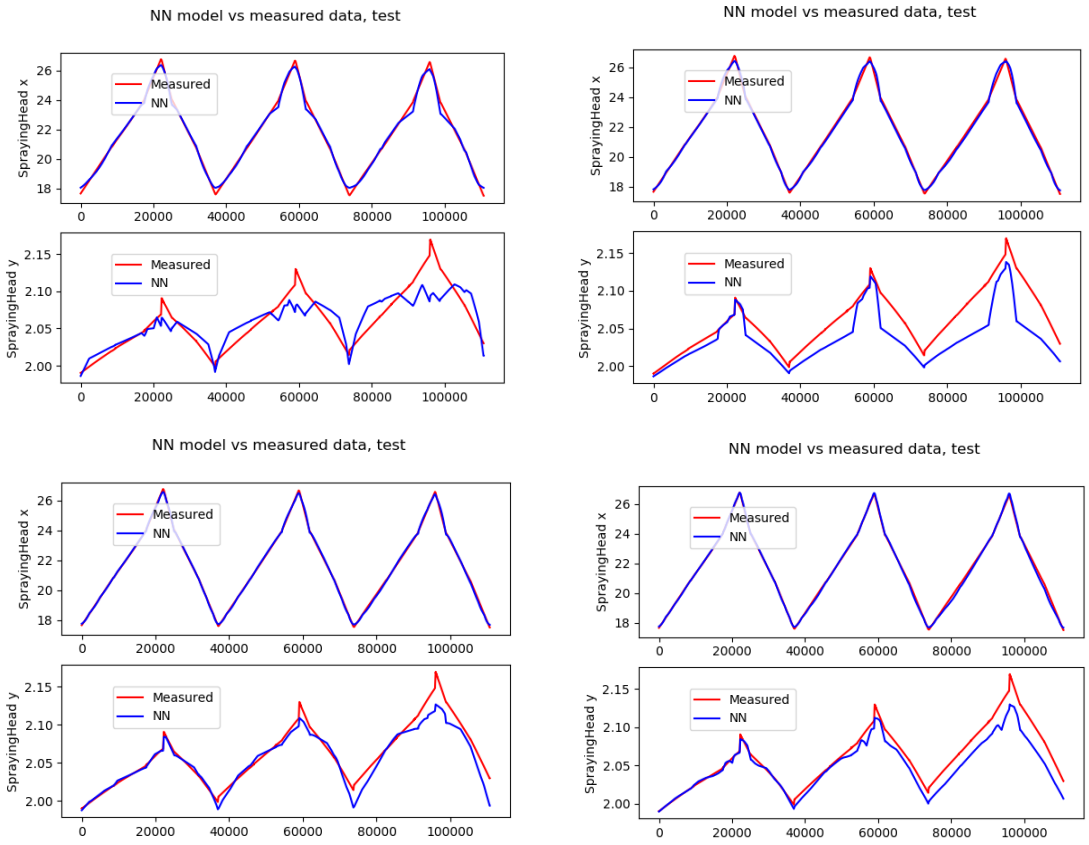


Figure 20. Test results for a neural network with 2 hidden layers with a varying number of nodes per layer. The first figure, top left, has 8 nodes per layer, top right has 16 nodes per layer, bottom left has 32 nodes per layer, and bottom right 64 nodes per layer.

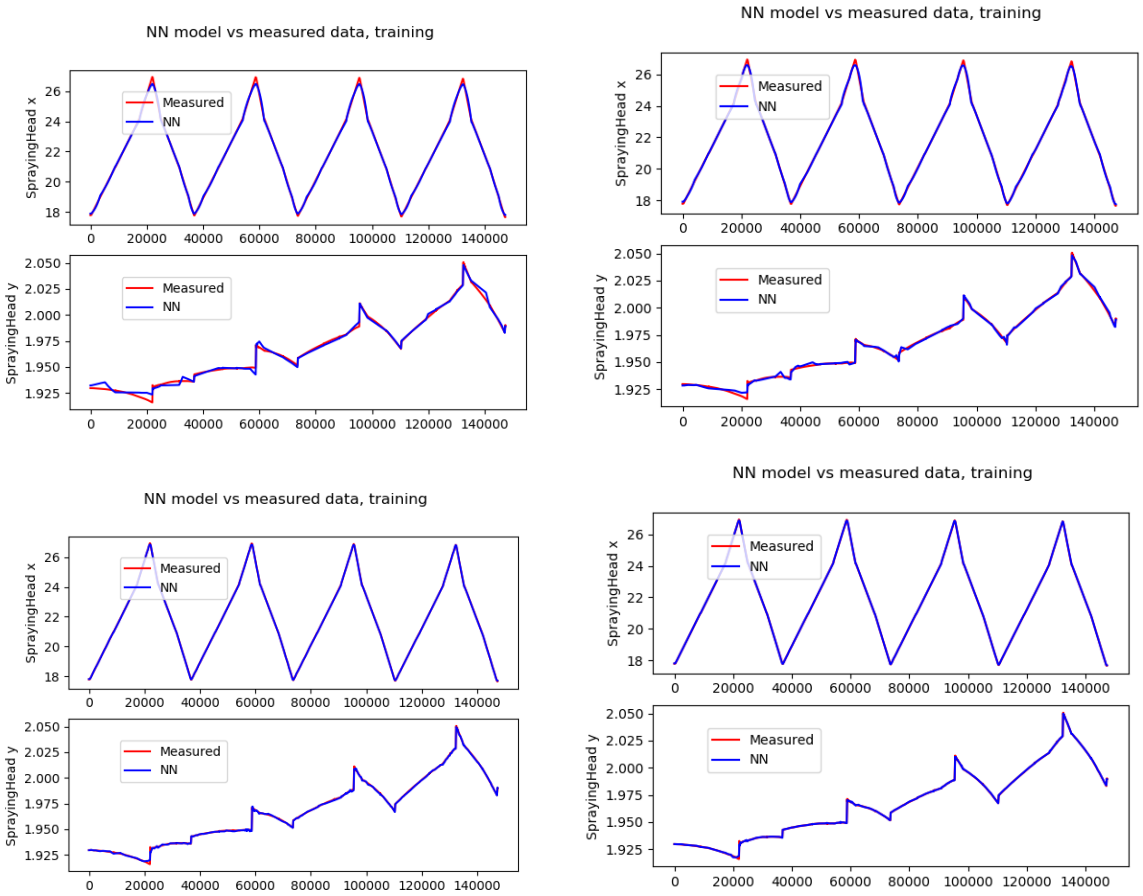


Figure 21. Training results for a neural network with 4 hidden layers with a varying number of nodes per layer. The first figure, top left, has 8 nodes per layer, top right has 16 nodes per layer, bottom left has 32 nodes per layer, and bottom right 64 nodes per layer.

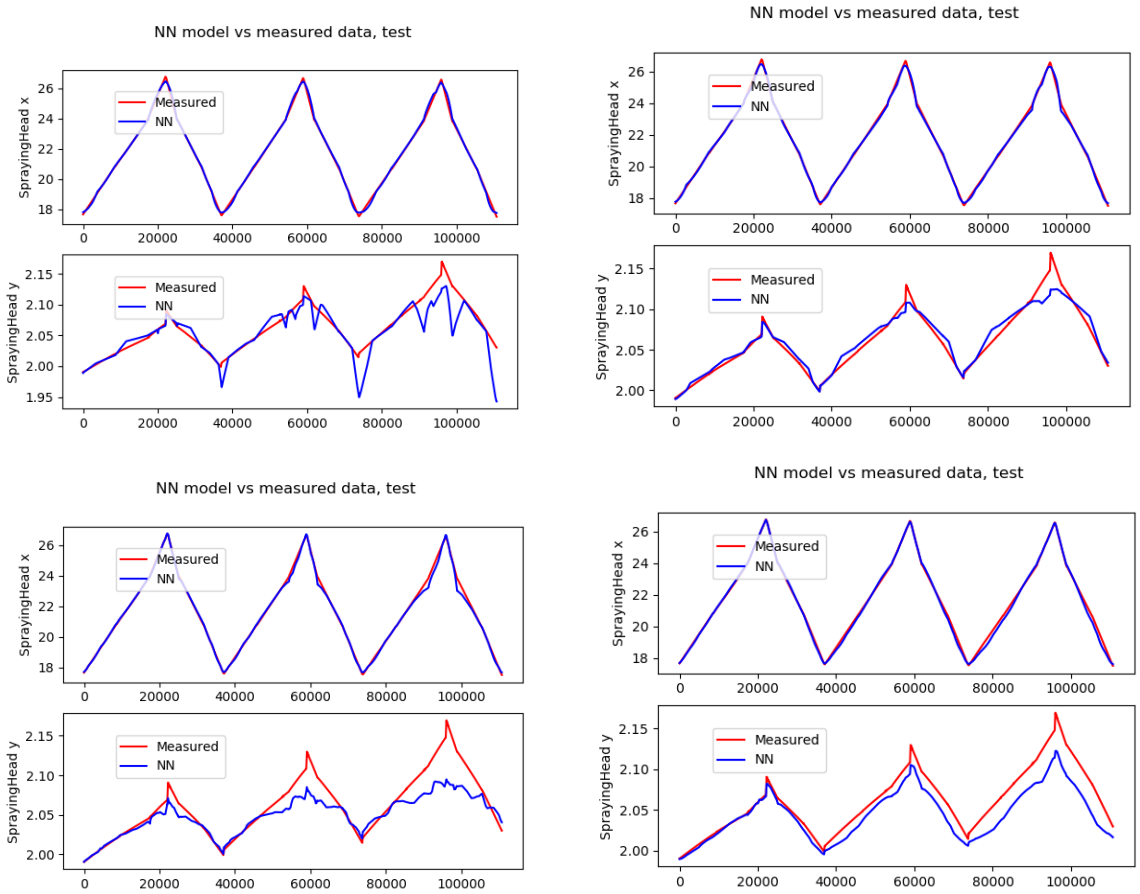


Figure 22. Test results for a neural network with 4 hidden layers with a varying number of nodes per layer. The first figure, top left, has 8 nodes per layer, top right has 16 nodes per layer, bottom left has 32 nodes per layer, and bottom right 64 nodes per layer.

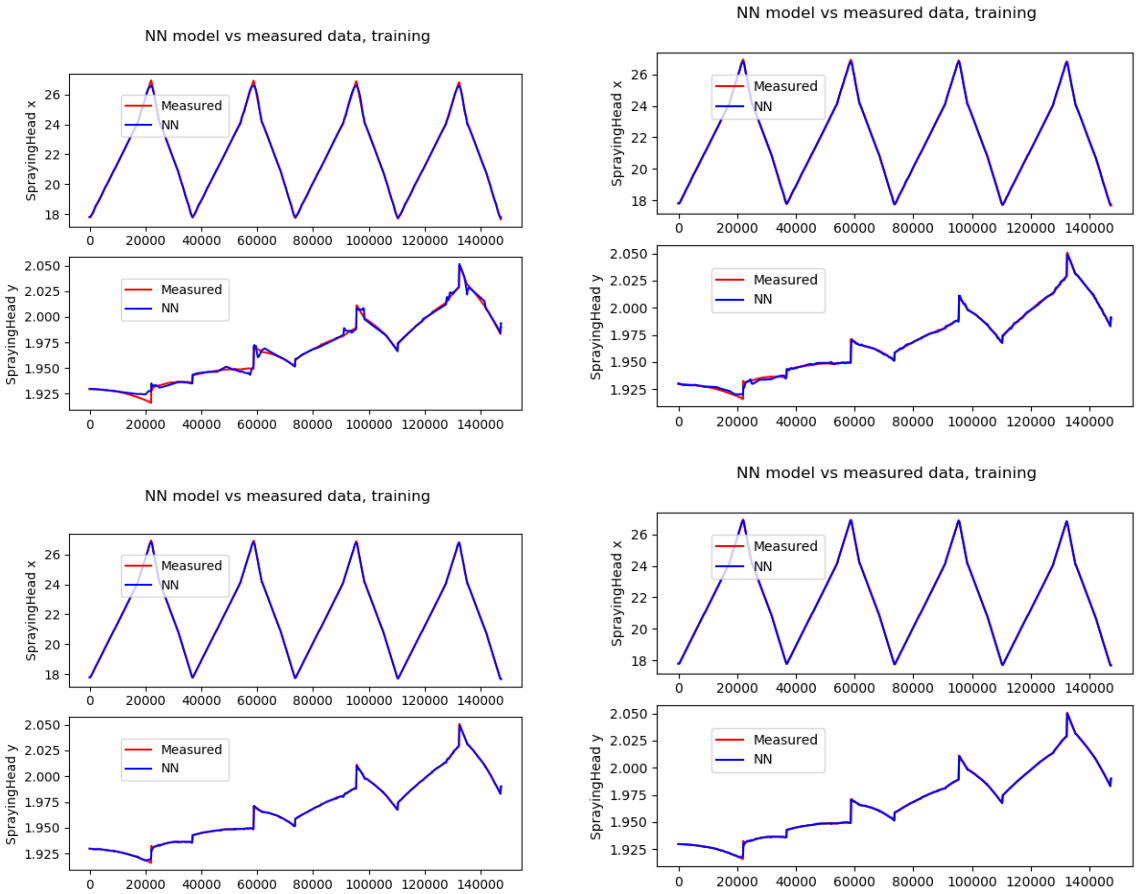


Figure 23. Training results for a neural network with 6 hidden layers with a varying number of nodes per layer. The first figure, top left, has 8 nodes per layer, top right has 16 nodes per layer, bottom left has 32 nodes per layer, and bottom right 64 nodes per layer.

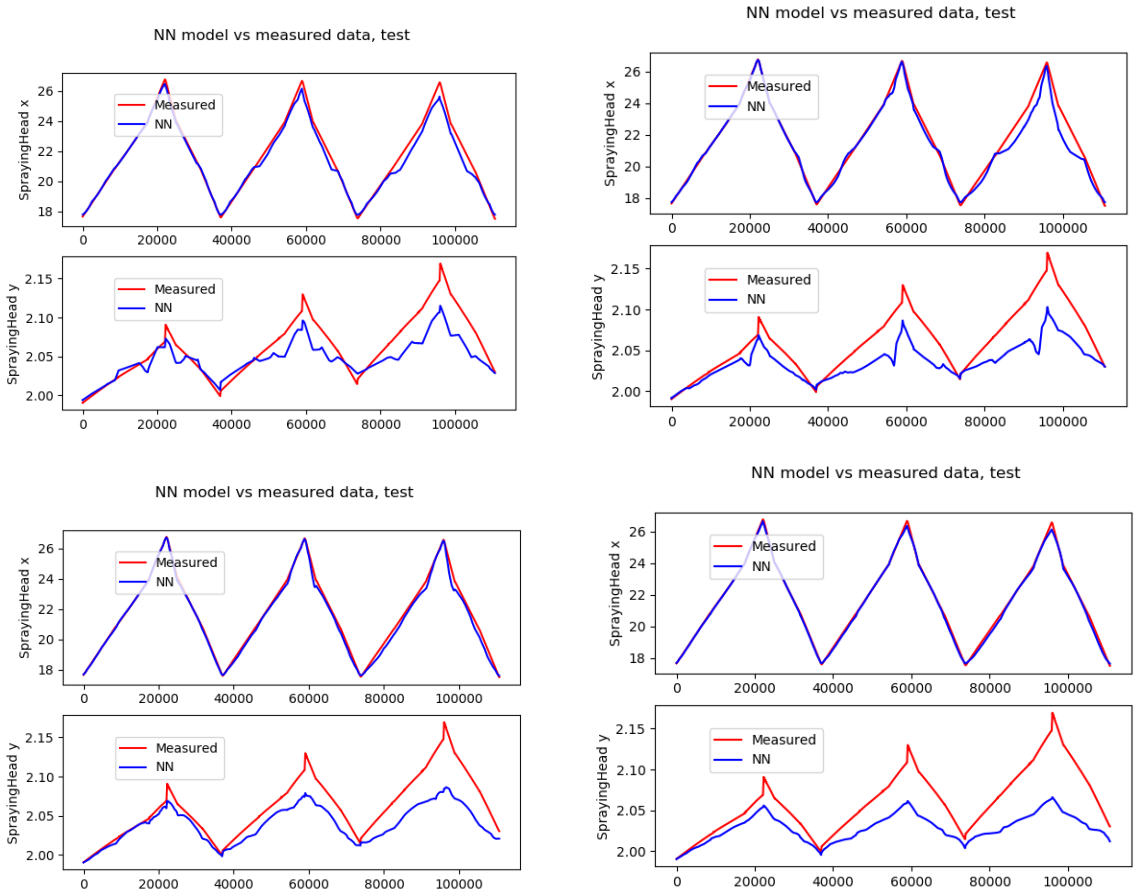


Figure 24. Test results for a neural network with 6 hidden layers with a varying number of nodes per layer. The first figure, top left, has 8 nodes per layer, top right has 16 nodes per layer, bottom left has 32 nodes per layer, and bottom right 64 nodes per layer.

Training and testing with data acquired from two separate simulator runs

The following figure shows the training and testing inputs acquired from two separate runs in the simulator. The testing inputs were acquired from a run were the Boom1_Lift had a +100 offset related to the training run. In the figure, the red graph represents the training data, and the blue graph the testing data.

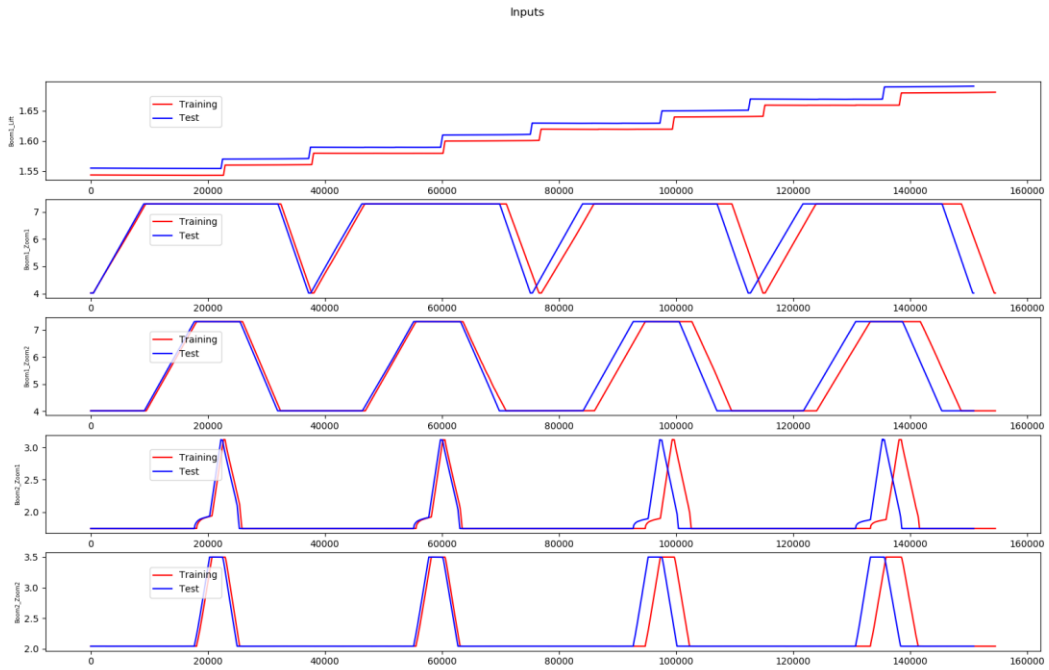


Figure 25. Unnormalized training and testing inputs.

The following figures show the training and testing results from a neural network that had 2 hidden layers and 64 nodes per layer.

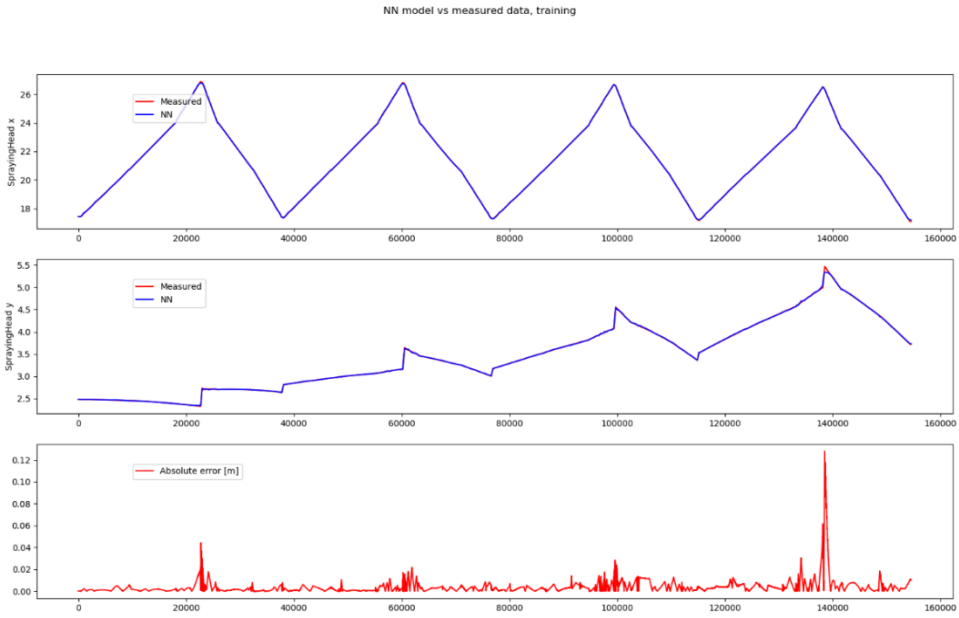


Figure 26. Training results from a neural network with 2 hidden layers and 64 nodes per layer.

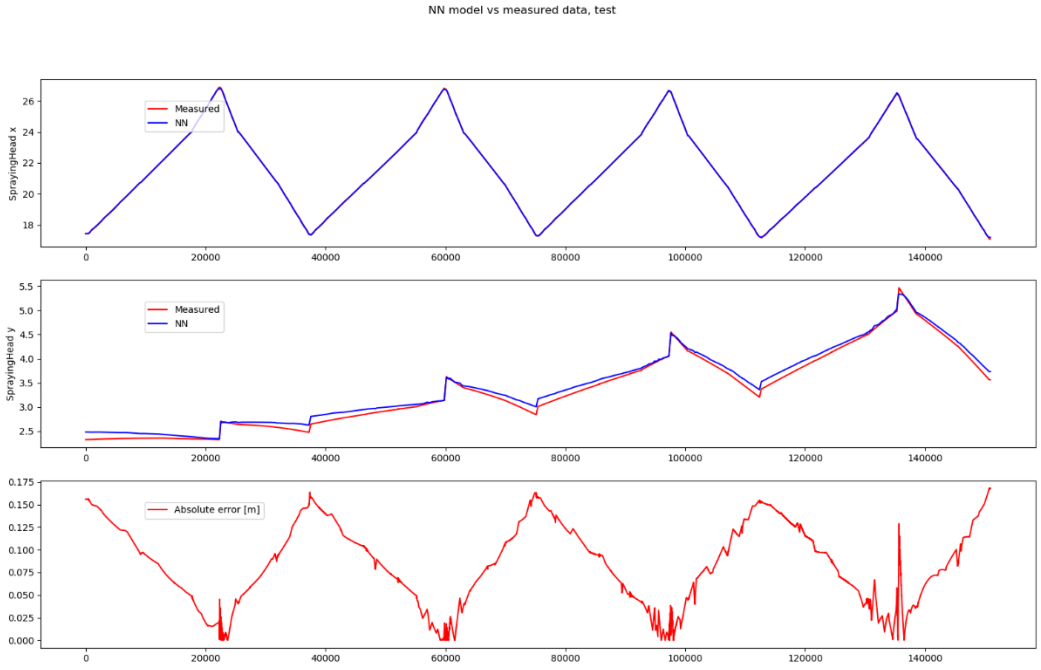


Figure 27. Testing results from a neural network with 2 hidden layers and 64 nodes per layer.

The testing results above show biggest errors when all the zoom cylinders are in and the lowest errors when the zoom cylinders are out. We do not know why the neural network gives the worst results when the zoom cylinders are in, when there are no deflections in the boom.

Conclusion and discussion

In conclusion, the neural networks seem to model the deflections quite well when the structure is fairly simple. The outputs given by the neural network are close to real values when the inputs stay close to the training data. The biggest question, however, is the error when the zoom cylinders are in in the last test case; this requires further work to determine the cause.

3.2.4 Boom deflection modelling with analytical methods

With a long boom, the elasticity of the structure as well as mechanical clearances can cause positioning errors. The position of the end effector is usually calculated based on measured joint positions by solving forward kinematics and all structures are assumed to be rigid. In practice, the position of the end effector hangs lower due to deflections and clearances. This error can easily be >30 cm when the boom is fully extended. To compensate this, we developed a Deflection model. The compensation is based on deflection equations of the supported beams and a kinematic model of the clearances. The developed model only takes static forces into account. The model can be solved in real time and could be used in boom control applications.
Description of the modelling method:

1. Boom structure is divided to three segments (Figure *28*).
2. Three zoom cylinders of the boom are modelled as beams supported from two points, and a free-hanging end section. At the end of the last segment there is a load. The load and moment caused by this are calculated for each segment separately based on beam deflection equations (Figure 29).
3. Load caused by the weight of each beam is taken into account as forces and moments affecting each segment.
4. Clearances of zoom cylinders are calculated based on the kinematic model (Figure 30). When the zoom cylinders are extended, the effect of the clearances increases as the distance between supporting points decreases.
5. Total deflection of the boom is calculated by combining segments and taking into account the slope angle of each segment. This slope angle is calculated from deflection equations and by adding the effect of clearances.

Initial values for the model are taken from the CAD model of the boom. These include dimensions of the links and masses. Moment of inertia, I, is calculated for each beam based on the cross section dimensions, and the modulus of elasticity, E, is a material-dependent constant. Since the beam model is very simplified expression of the real boom structure, the model parameters need to be tuned experimentally.

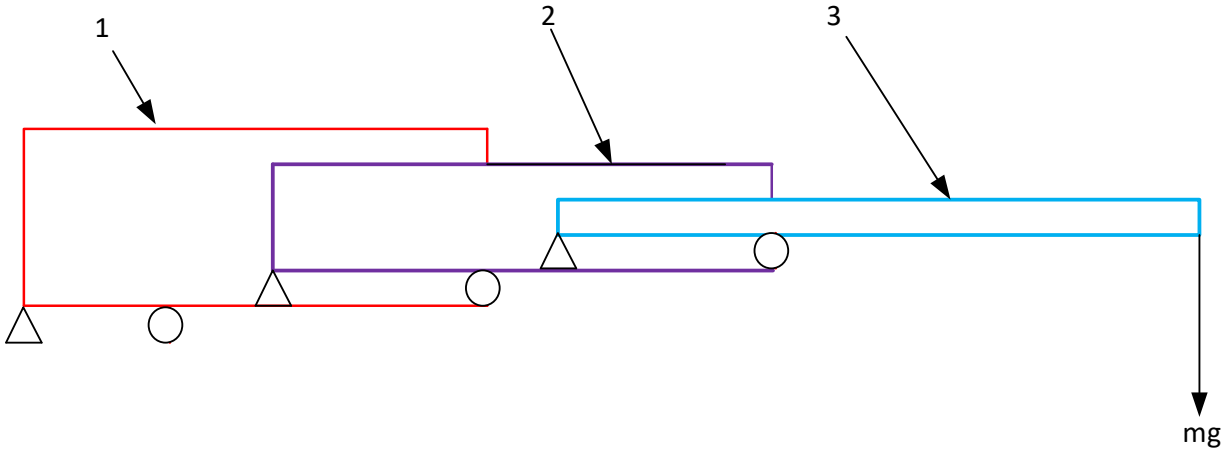
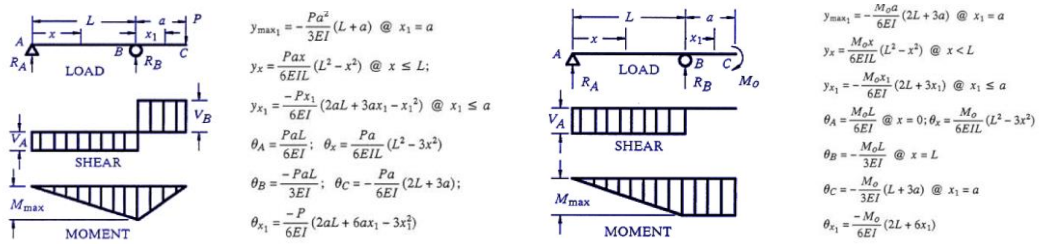


Figure 28. *Boom consisting of three zoom cylinders (1-3).*



Young, W. C., Budynas, R. G.(2002). Roark's Formulas for Stress and Strain . 7nd Edition, McGraw-Hill.

Figure 29. Load cases: force at end of beam (left) and moment at end of beam (right).

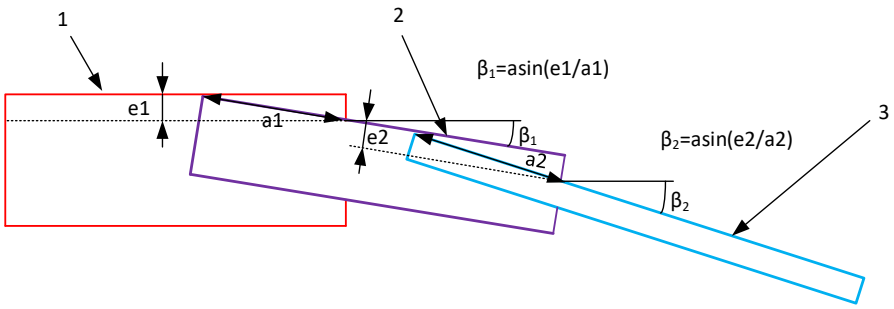


Figure 30. Clearance model.

Deflection modelling was done with Matlab software. The shape of the boom is calculated as a function of the position of the zoom cylinders of the boom. In the deflection model several parameters (etc. clearances *e1* and *e2*, loads, beam cross sections, modulus of elasticity *E*) can be varied. As an example, in Figure 31 the shape of the boom is calculated when the two zoom cylinders are fully extended to 3300 mm. With the parameters used, the maximum deflection is 115 mm at the end of the boom.

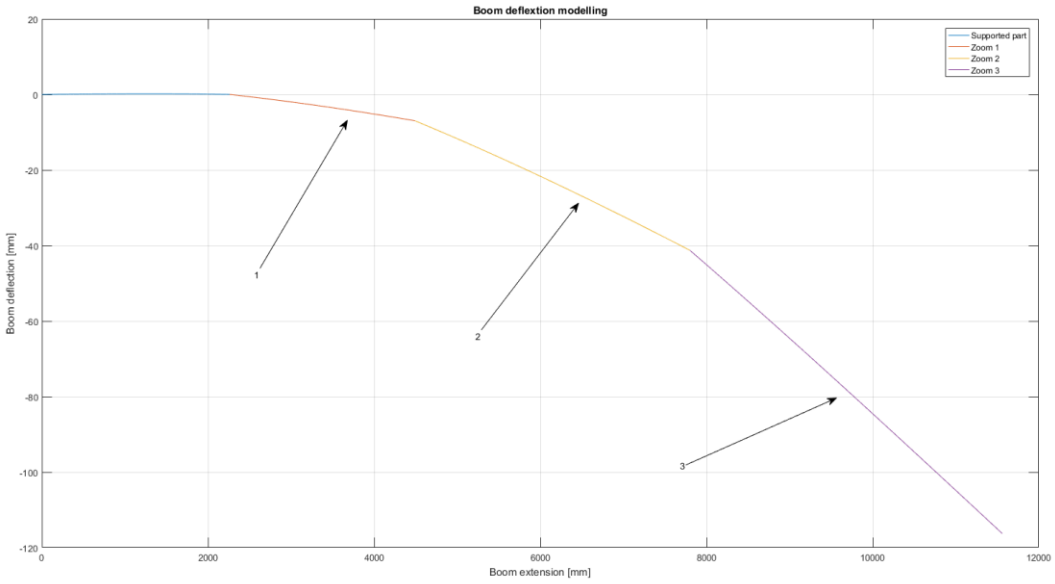


Figure 31. Example of the calculated shape of the boom.

Measuring deflections of a real boom

Deflections of a real boom were measured using the test setup presented in Figure 32. The test setup consisted of a magnet-mounted laser beam transmitter (A), which was attached to the first part of the boom. This laser beam forms a reference. Scale (B) is attached to the zoom of the boom with a magnet. The laser beam forms a visible line that can be read from the scale. When the zoom is extended using the hydraulic zoom cylinders, the deflection of the boom increases. With this setup, the deflection at the end of the boom was measured at different cylinder positions. The measurement method is relatively simple. A key drawback is that the elasticity of the beams cannot be distinguished from the effect of the structural clearances of the boom. Also, any error in parallelism of the laser beam and the first boom section will affect the measurements.

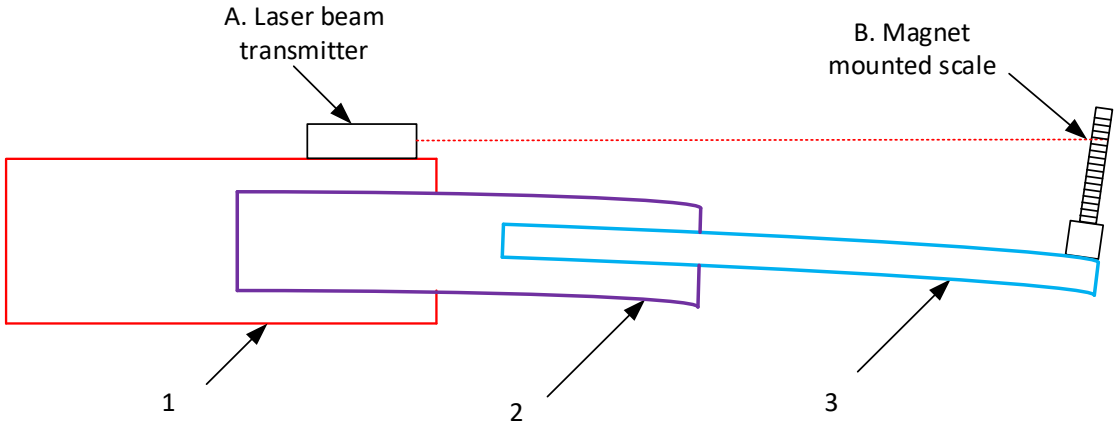


Figure 32. A method for measuring boom deflection using a laser beam transmitter.

Comparing measured and calculated deflections

In Figure 33, measurements at different positions of the zooms are compared to the values calculated using the deflection model. The deflection model parameters were selected so that the maximum deflection value matches the actual measurements. The model matches the measurements better when both zooms cylinders are extended simultaneously (red markers). In general, the values calculated with the deflection model (blue markers) are within ±20 mm of the measured values. When moving only one zoom cylinder and keeping the other zoom cylinder at the zero position (green and cyan markers), the accuracy of the model decreases. A potential reason for this is that selected modelling method (load cases and clearance model) represents the actual situation better when both zooms cylinders are extended over half of their movement range.

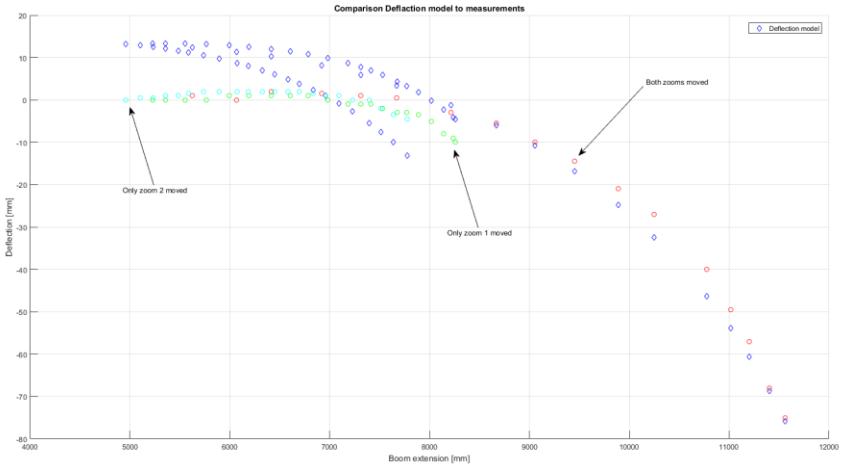


Figure 33. Deflection model (blue markers) vs. measurements from the real boom (red, green and cyan markers).

Conclusion and discussion

The developed method only takes into account gravity and the clearances of the zooms cylinders. Based on the measurements, the method could still be useful in reducing the positioning error of the end effector of the boom. The challenge is to measure the deflections of the real boom and adjust the model parameters accordingly.

4. Ensuring machine safety

Machine safety and cyber security are both associated with risks, and risk assessment is an essential tool for both. However, the risks originate from different sources. Safety risks are related to the probability of random or design failures, whereas cyber security is typically related to malicious human actions, where the weakest link dominates. Risk mitigation is, in both cases, related to design, but whereas safety is focused on the design of the machine manufacturer, cyber security is associated with various actors. Currently, safety and cyber security require separate risk analyses, as it would be too laborious to consider all risks from both the machinery safety and cyber security point of view.

We developed a PL (Performance Level) calculation tool to support functional safety calculations. Several features, such as SIL calculation, documentation, structure visualization and updates to standard requirements, were added to the original tool. The tool is designed for the calculation of PL and PFH (Probability of dangerous Failure per Hour) in the early phase of design when not all components are yet fully defined. The tool can give minimum requirements for the missing components. It can also be applied when all components are known and summary documentation is needed.

This section presents three strategies for designing safety features for autonomous mobile machine fleets: 1) Rules-based strategy for an automated area, 2) Area isolation, and 3) Safe separation distance. Each strategy brings a different level of safety and accessibility to the system. Currently, area isolation often gives the best safety level and high productivity, but there can be difficulties related to large isolation areas and realizing human actions in isolated areas. On-board safety systems are associated with safe separation distance and require excellent control of speed, position and object detection. On-board safety systems operate well in indoor applications, but outdoor applications require reliable sensors for demanding environments and longer detection ranges. Sensor technologies are expected to develop in the near future to meet the requirements of at least some outdoor conditions. The rules-based strategy for automated areas is a human-dependent approach to increasing safety. In most cases it is not an adequate strategy for use alone. Traffic safety is highly dependent on the ‘rule of the road’ and it is evident that only a certain level of safety can be achieved with human actions.

Li-ion batteries can reach a self-heating stage that can lead to thermal runaway. All of the components needed for fire are present in the Li-ion cell: fuel, heat and oxygen. In addition, large amounts of hazardous gases are produced during Li-ion battery fires. The most significant gases are the emissions from hydrofluoric and hydrochloric acids. The most common way to deal with a Li-Ion battery fire is to apply plenty of water, both to extinguish the fire and to cool the battery to avoid further battery self-ignition. The battery pack should be designed in a way that makes it possible to effectively cool overheated battery cells. Container-like battery pack protection significantly decreases the amount of water needed and provides an effective way to cool an overheated battery without risk of re-ignition. To ease the work of first responders, machine type specific instructions should be prepared. The instructions should also guide operators in identifying a battery fire.

4.1 Risk assessment of machine systems with respect to safety and cyber security

This section is related to VTT Research Report VTT-R-01428-18: Risk assessment of machinery system with respect to safety and cyber security.[16]

Definitions:

1. Cyber security: Measures taken to protect a computer or computer system against unauthorized access or attack.[17]

2. Functional safety: Part of the safety of the machine and the machine control system which depends on the correct functioning of the safety-related electronic control system, other technology safety-related systems and external risk reduction facilities.[18]

The machinery sector has a long tradition in risk assessments and addressing safety issues. Currently, risk assessments are typically carried out according to ISO 12100[19] or, if the focus is on control systems, according to ISO 13849-1[20]. Cyber security issues have gained public awareness mainly due to the threats associated with costs and confidentiality. Clearly, security can also affect safety, and interest in security issues has risen among machine builders. This section addresses cases where cyber security may affect machine safety. There are already several standard proposals related to the connection between cyber security and safety, but the field is still evolving. The idea is that security issues must not threaten safety, but on the other hand, the required resources must be in line with the risk.

This section specifically addresses the need to combine risk assessments to cover both safety and related cyber security issues. The security issues covered in this case are limited to safety functions of control systems, communication, safety of machinery misuse (interfaces) and other safety-related situations that are rare, but possible. The information for this report has been collected from standards and draft standards. Cyber security information is drawn mainly from draft standards, as few standards related to cyber security have been formulated.

Safety-related risk is a function of severity and probability, whereas security risk is a function of negative impact and likelihood. While there are similarities between the two, security risks are more difficult to quantify. Safety risk is usually related to random events, whereas security risk relates to purposeful acts. This means that the probability of vulnerability exploitation due to random events can be low, but if vulnerabilities are exploited purposefully, the probability is not applicable. Security risk may change as technologies or circumstances change, but it does not disappear and a long use history does not necessarily guarantee a secure system. There are some similarities between software and cyber security validation. Safety software validation is often related to analyses, inspections, walkthroughs, design processes and testing in many phases of design against safety and functionality requirements. Validation of the cyber security of software is more related to how threats, vulnerability and assets are treated against target security levels (SL-T) and other cyber security requirements.

[16] Malm T., Ahonen T., & Välisalo T. Risk assessment of machinery system with respect to safety and cyber-security. VTT-R-01428-18. 26 p.
[17] ISA/IEC 62443-3-2: 2017 draft. Security for industrial automation and control systems -Security risk assessment, System partitioning and Security levels. 36 p.
[18] SFS-EN 62061. 2005. Safety of machinery – Functional safety of safety-related electrical, electric and programmable electronic control systems. 198 p.
[19] SFS-EN ISO 12100. 2010. Safety of machinery. General principles for design. Risk assessment and risk reduction. Finnish Standards Association SFS. 172 p.
[20] SFS-EN ISO 13849-1. 2015. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design. Finnish Standards Association SFS. 193 p.

The IEC/ISA 62443 series of standards suggest that there should be target security levels[21] [22] [23](SL1-SL4) that specify the general risk level and the target in order to quantify countermeasures against cyber security risks. There is some similarity between Safety Integrity Levels (SIL according to IEC 61508 and IEC 62061[24]) and Performance Levels (PL according to ISO 13849-1[25]), which are applied to measure safety risk and related protective measures of machinery safety functions. The mentioned standards are related to automation and control systems. In that field, there is a need to compare risks and risk reduction measures in order to direct resources according to the risk levels.

The classification of functional safety is relatively mature. The categories of machinery control systems (currently part of PL determination) were introduced in 1996 (EN 954-1), SILs in 1999 (IEC 61508-1) and PLs in 2007 (ISO 13849-1). The history of safety classification dates back to the 1980s and the development of IEC 1508 and some national standards (Germany and UK). Currently, there is a development move towards merging SILs and PLs, but this is challenging. Security levels were introduced in 2009 (IEC/TS/ISA 62443-1-1), but are apparently not yet applied as widely in automation as SILs or PLs.

One aspect of the relation between safety and cyber security risks is that, according to the Machinery Directive (2006/42/EC)[26], the machine builder (or authorized representative) must consider in risk assessment the ‘intended use and any reasonably foreseeable misuse thereof’. Many cyber security risks may be associated with ‘reasonably foreseeable misuse’. The Machinery Directive relates to safety, but since cyber security can affect safety, it should also be considered.

Although risk assessment from the safety and security points of view have many similarities, it is still difficult to integrate security risk assessment with safety risk assessment. Many safety requirements are obligatory, but from the safety point of view measures against security risks are voluntary unless there is a clear connection with a safety issue, e.g. reasonably foreseeable misuse. Without a systematic approach combining safety and security, it can be difficult, for example, to determine whether given security issues have an effect of safety. The current paper contributes to the development of an integrated approach and examines its pros and cons. As a brief overview, safety and cyber security can be considered to have:

- Independent domains: dealt with by separate persons.
- Little interaction: similarities in risk reduction are not taken into account.
- Common infrastructure: safety and security issues are related to the same devices.
- Conflicting responsibilities? In many cases different persons are controlling the domains and responsibility of the entity is not clear.

Suzuki describes the relationship between security, safeguards and safety in the nuclear industry[27]. Figure 34 illustrates how security, safeguards and safety are positioned in relation to axes of frequency and law. It also describes how probabilistic means are applied to estimate different situations. The figure has heuristic features, as Suzuki mentions, yet there

[21] ISA 62443-1-1: 2017. Security for industrial automation and control systems. Models and concepts. 114 p.
[22] ISA/IEC 62443-3-2: 2017 draft. Security for industrial automation and control systems -Security risk assessment, System partitioning and Security levels. 36 p.
[23] ISA/IEC 62443-3-3: 2013. Security for Industrial automation and control systems. Part 3-3: System security requirements and security levels. 81 p.
[24] SFS-EN 62061. 2005. Safety of machinery – Functional safety of safety-related electrical, electric and programmable electronic control systems. 198 p.
[25] SFS-EN ISO 13849-1. 2015. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design. Finnish Standards Association SFS. 193 p.
[26] Machinery Directive 2006/42/EC. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). 63 p.
[27] Suzuki, Mitsuo. 2018. Integrated Risk Assessment of Safety, Security, and Safeguards. In: Risk assessment. Ed. Svalova, Valentina. Pub. InTech. pp. 133-151. ISBN 978-953-51-3799-3.

are historical incidents (35 incidents) behind it. Security incidents have been rarer than safety incidents, but severe safety and security incidents are rare.

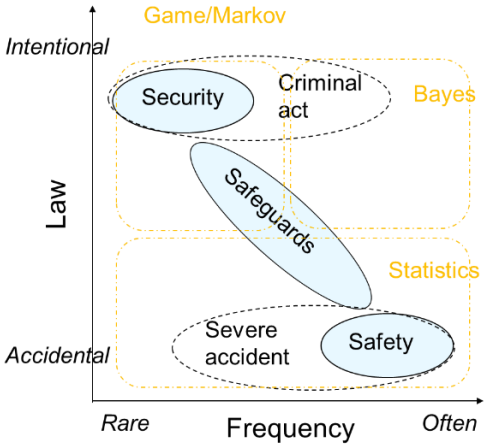


Figure 34. Relationship between security, safeguards and safety (Suzuki).

The objectives related to machinery safety and cyber security risk assessment are described in Table 1. A comparison of functional safety and cyber security is presented in Table 2.

Table 1. Principle objectives of machinery safety and cyber security.[28]

	Machinery safety	**Cyber security**
Objectives	Injury/accident prevention, health (avoidance of harm)	Availability, integrity, confidentiality
Conditions (risks, methods, measures)	Transparent (not confidential)	Confidential (not shared with machinery user)
Dynamics	Rather static field (intended use, reasonable foreseeable misuse)	Highly dynamic field; moving target (intentional manipulation, criminal intent)
Risk property	Risk is often related to random events or software properties	Risk is often related to deliberate, malicious human actions
Risk reduction (mitigation) measures	Mainly by machine manufacturer at a dedicated time (when providing the machine for first use)	By various actors (machine manufacturer, system integrator, machine user, service provider) at any time throughout the life cycle.

Table 2. Comparison of functional safety and cyber security[29].

Life cycle phase		**Functional safety**	**Cyber security**
Risk analysis	Type of evaluation	Equipment under control	Zones and conduits based on logical grouping of assets
	Failure likelihood	Random failures due to operational and environmental stress.	Threats: internal, external or combination. Vulnerabilities due to

[28] ISO/DTR22100-4 proposal: 2018. Safety of machinery – Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects. 15 p.
[29] ISA 62443-1-1: 2017. Security for industrial automation and control systems. Models and concepts. 114 p.

Life cycle phase		Functional safety	Cyber security
		Systematic failures due to errors during safety life cycle.	- component or system design flaws - making non-valid changes - not following security practices and procedures - threats exploiting vulnerabilities leads to failure
	Consequence severity	Impact on environment health and safety of personnel and the general public.	Loss of availability and/or data integrity has direct impact and loss of confidentiality has indirect impact on functionality
	Risk categorization	Based on likelihood and severity; risk may be quantified.	Based on likelihood and severity, risk is currently qualitative. Risk categorization for every security requirement. Multi-dimensional problem Assigned to zone with target SL for each zone/conduit.
	Risk mitigation measures	Relies on independent protection layers concept. Safeguards reduce likelihood of consequence evaluated. Identifies integrity requirements for safeguards; for safety function assigns target SIL.	Relies on security counter measures within zone, within conduits connected to the zone, and defence in-depth concept. Countermeasures reduce likelihood. Identify requirements for countermeasures to meet the zone target SL for each threat vector.
Implementation measures		Safety manual for components. Quantitative SIL verification for safety functions	Security manual for components. Verification through different levels of testing for target SL.
Operation and maintenance		Restrict access to control system components to competent personnel with necessary access privileges. Periodic testing of measures. Demand rate and component failures to be monitored. Awareness and training.	Restrict access to control system components to competent personnel with necessary access privileges. Periodic testing of measures. Frequent reviews to identify new vulnerabilities and take appropriate action as necessary. Awareness and training. Cyber risk reassessment after each software or hardware change.
Management system		Defines requirements for competency, training, verification, testing, audit and documentation.	Defines requirements for competency, training, verification, testing, audit and documentation.

The safety and cyber security risk assessment and risk reduction process can be presented in block diagram format to reveal mutual phases. Similarities can be found also by looking attributes or properties of software.

Figure 35 shows a mind map of cyber security and functional safety. The figure shows the main connections between the two domains. Cyber security is violated through assets associated with design and systematic (software) failures, and the cause is related to threat and vulnerability. Functional safety risk is associated with inherently safe system and safety function failure. Safety function failure means that the function is silent or its performance is hazardous. Furthermore, the reasons for safety function failure are usually integrity, availability or response time change, which are initiated by software, design or hardware failures. The asset (see definition) can be associated with software and hardware, but here, since hardware failures are more associated with functional safety, no direct connection is drawn between them. Misuse prevention and deliberate human initiated attack may have some mutual aspects, such as authentication, use control and encryption.

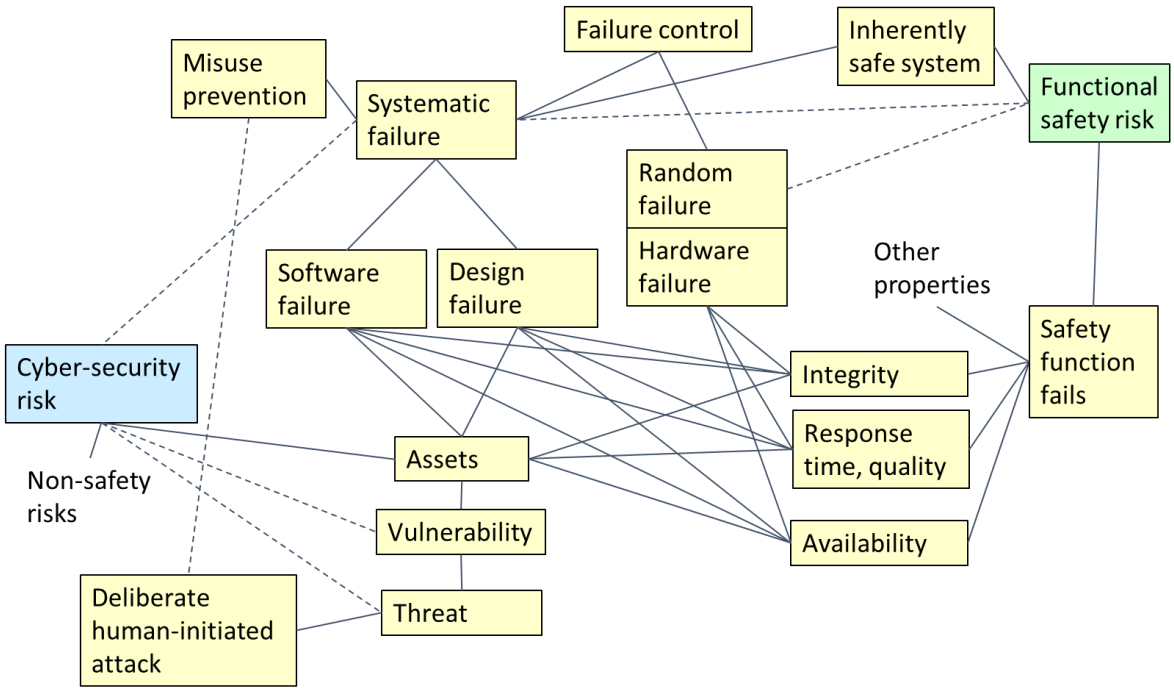


Figure 35. Mind map of cyber security and functional safety.[30]

An important issue related to control system and cyber security risks is classification. The means of minimizing risks can be categorized according to the type of risk and its corresponding requirements. These requirements depend on the required rigor and extent of risk minimization. Security levels are presented in
Table **3**. The functional safety classification (PL and SIL) is described in Table 4 and Figure 36.

[30] Malm T, Ahonen T & Välisalo T. Risk assessment of machinery system with respect to safety and cyber-security. VTT-R-01428-18. 26 p.

Table 3. Security levels.[31]

Security level	Description
SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means with low resources, generic skills and low motivation
SL 3	Protection against intentional violation using sophisticated means with moderate resources, IACS (Industrial Automation Control Systems) specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation.

4.2 Approach and tool for safety function PL calculations

4.2.1 Changes to safety requirements of control systems

Safety requirement are developing in several levels. New version of Machinery Directive (MD) is planned to be published at 2021[32]. The aim of the revision is to tackle possible challenges that may arise from technical progress in digitisation. The Inception Impact Assessment of MD mention following new topics[33]: IoT (Internet of Things), AI (Artificial Intelligence), new generation of autonomous robots and cyber-security.

Harmonized standard, is presumed to comply with the essential health and safety requirements covered by such a harmonized standard[34]. During 2019 the role of harmonized standards has changed. Earlier harmonized standards were published in Official Journal C series (associated to competition, resolutions, recommendations, and opinions) and now they are published in L series (legislative acts). This means that harmonized standards have now a stronger status. Currently part of harmonized standards are in C series and new standards are in L series. In the future the harmonized standards need to describe more precisely the relation to the Machinery Directive and all current harmonized standards are not going to keep their status. Standards like SFS-EN ISO 13849-1 and SFS-EN 62061 are supposed to keep their status when new versions are published.

The functional safety standards for machinery will be published according to plans about 2021 (first IEC 62061 and later ISO 13849-1). There have been a lot comments to the revision of ISO 13849-1 and for example software requirements have first changed a lot, but later the changes have been removed. So, it is difficult know in current CD2 phase, what the final changes will be. Anyway, major changes are difficult to become approved and therefore presumably the changes will be rather large, but only in details.

Safety logics is mentioned at MD Annex IV and they need to be type examined (actually type-examined according to MD Annex IX, internal checks according to MD Annex VIII or full quality assurance according to MD Annex X) if they fulfil also safety component definition:

[31] ISA/IEC 62443-3-2: 2017 draft. Security for industrial automation and control systems -Security risk assessment, System partitioning and Security levels. 36 p.
[32] EU. Machinery Directive -revision website. https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-6426989_en
[33] EU. Machinery Directive -revision website.
[34] Machinery Directive 2006/42/EC. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). 63 p.

"Safety component means a component, which serves to fulfil a safety function, which is independently placed on the market, the failure and/or malfunction of which endangers the safety of persons, and which is not necessary in order for the machinery to function, or for which normal components may be substituted in order for the machinery to function."[35]

The standard IEC 61131-6 Programmable controllers – Part 6: Functional safety is related to safety logics (no progress is going on the standard). Its scope describes that application specific information needs to be achieved from IEC 62061 or ISO 13849 series and safety integrity level capability may not be greater than SIL 3. The standard is not harmonized and therefore it does not comply with the essential health and safety requirements of MD although its scope is related to functional safety of programmable controllers. Therefore the standard should be applied together with harmonized standard (IEC 62061 "Functional safety of safety-related electrical, electronic and programmable electronic control systems" and/or ISO 13849-1 "Safety-related parts of control systems").

4.2.2 Functional safety

Functional safety relates to the safe performance of actuators when a specified safety function is initiated by a safety-related control system. A safety function or safety-related function can fail due to a random failure or a systematic failure and the system needs to have means to perform safety function in spite of failures or the probability of the failures need to be very small. The probability of dangerous failure determines the capability of the safety function (see SIL and PL in Table 4).

In the machinery sector, the harmonized functional safety standards are ISO 13849-1[36] and IEC 62061[37]. Both standards refer to IEC 61508 series of standards: Functional safety of electrical/electronic/programmable electronic safety-related systems, which set the basis for the functional safety of programmable electronic systems. Table 4 shows the relationship between PL and SIL.

[35] Machinery Directive 2006/42/EC. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). 63 p.
[36] SFS-EN ISO 13849-1. 2015. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design. Finnish Standards Association SFS. 193 p.
[37] SFS-EN 62061. 2005. Safety of machinery – Functional safety of safety-related electrical, electric and programmable electronic control systems. 198 p.

Table 4. Relationship between PL and SIL (ISO 13849-1).

Performance level (PL)	Probability of dangerous failure per hour [1/h]	Safety integrity level (SIL)
a	$10^{-5} \leq PFH_d < 10^{-4}$	-
b	$3 \cdot 10^{-6} \leq PFH_d < 10^{-5}$	1
c	$10^{-6} \leq PFH_d < 3 \cdot 10^{-6}$	1
d	$10^{-7} \leq PFH_d < 10^{-6}$	2
e	$10^{-8} \leq PFH_d < 10^{-7}$	3

The safe performance design of control systems begins with risk assessment. When the risk is considerable and the control system (including electrical safety/protective devices) is required to maintain safety, then PL estimation is required. The performance level (PL) of the safety function is associated with the safe operation of machine functions. The PL is defined in standard ISO 13849-1. High risks related to the safety function mean more specific requirements. Figure 36 shows the process of how PL is defined and then realized and validated. The achieved PL must be at least the same as the required PL. Figure 36 shows the design process and how PL relates to it.

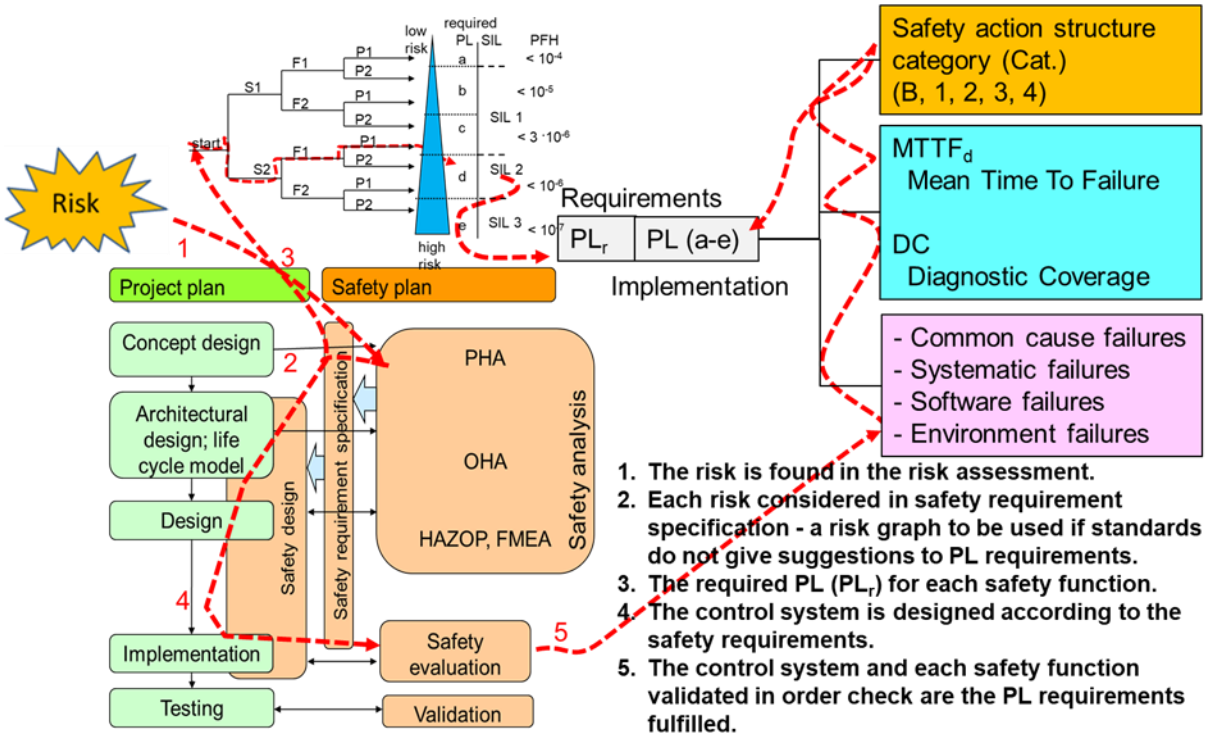


Figure 36. Basic procedure for meeting the functional safety requirements of standard ISO 13849-1.[38]

[38] Malm T, Heikkilä T & Ahola J M. Safety Assessment Process for Human-Robot Handling Tasks. 2015 ASME/IEEE International Conference on Mechatronic and Embedded Systems and Applications (MESA), August 03-05, 2015, IDETC/CIE 2015, Boston, USA

Safety block diagrams and categories

A safety block diagram for each safety function to be estimated is created based on the characteristics of the safety function. The safety block diagram interprets the architecture of the safety function. Note that this is not the same as a functional block diagram. A safety block diagram shows the redundancy of the safety function and may contain preventive components that are not directly related to functionality (e.g. fuses, pressure limiting valves). Five designated architectures are presented in ISO 13849-1 which fulfil specific design criteria and behaviour under fault conditions. These designated architectures can be utilized in creating safety block diagrams for the safety functions of a machine control system.

The categories can be associated with architecture and performance in a case of a failure. Figure 37 shows the designated architectures for which the standard provides calculated results according to Markov models for the designated architectures. The figure also roughly shows the associated PL and PFH typical for each category.

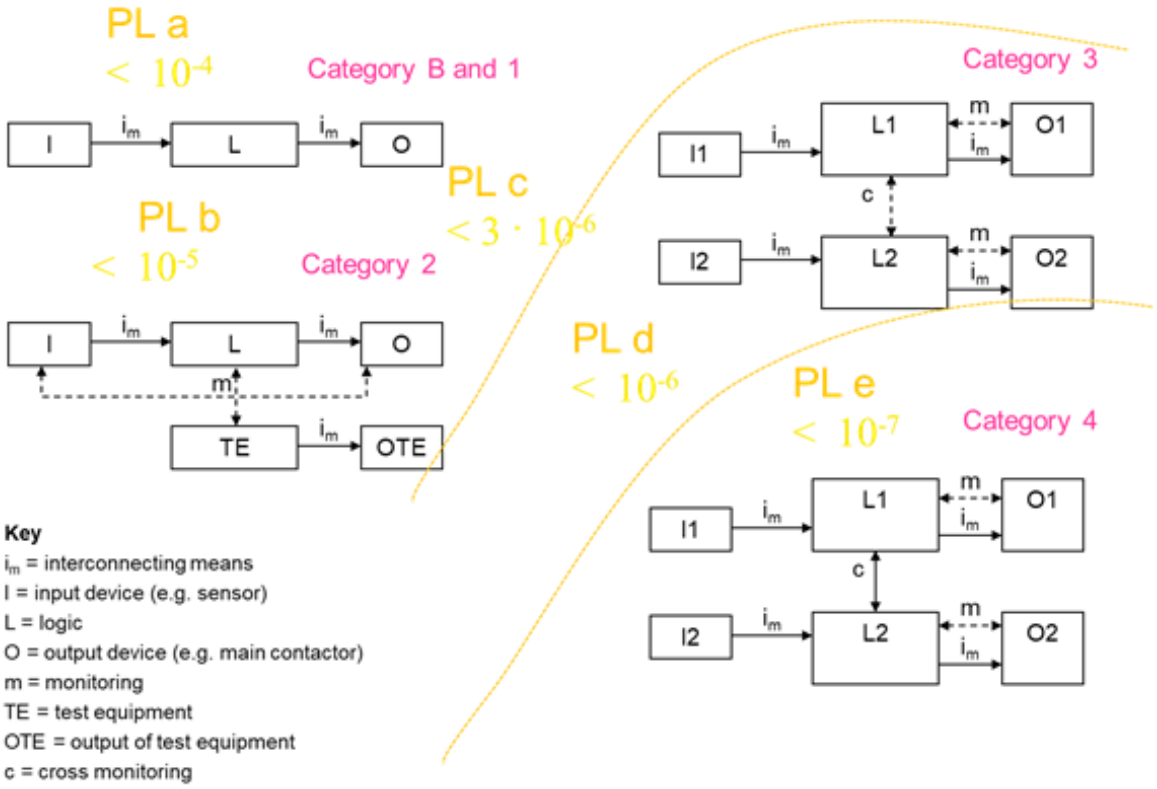


Figure 37. Designated architectures and related PLs according to ISO 13849-1[39].

$MTTF_D$ and DC

Once safety block diagrams have been created for the safety functions, the failure rate for each channel is calculated using the mean time to dangerous failure ($MTTF_D$) values of components and diagnostic coverage (DC) for failures.

Diagnostic coverage (DC) is a measure of the effectiveness of diagnostics. It can be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures.

[39] SFS-EN ISO 13849-1. 2015. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design. Finnish Standards Association SFS. 193 p.

PL estimation

When the levels for $MTTF_d$ and DC have been defined for all parts a safety function, the attainable PL for this safety function can be defined based on the graph in Figure 38. For category 2, 3 and 4 safety functions, common cause failures (CCF) need to be estimated. In addition to CCF, the requirements presented for software and measures against systematic failures need to be considered to complete the PL estimation.

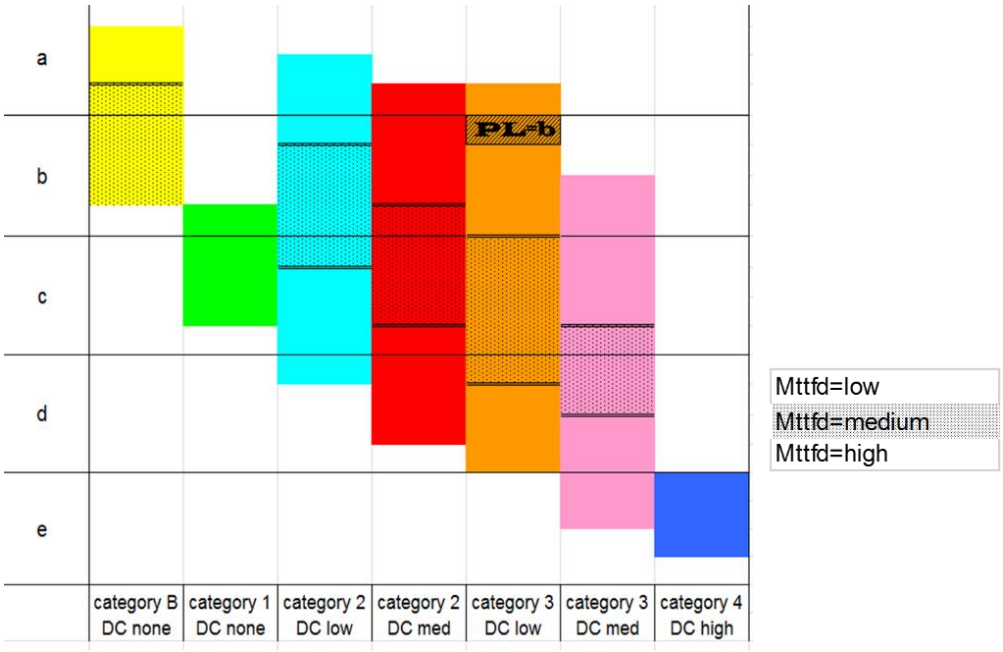


Figure 38. Subsystem result of the PL calculation tool.

4.2.3 PL Calculation tool

The original PL calculation tool or KOTOTU calculation tool was developed at VTT during the KOTOTU project (Koneiden ohjausjärjestelmien toiminnallinen turvallisuus) in 2009. It was funded by VTT, a group of partner companies, and the Work Environment Fund. The tool has since been modified in several projects at VTT. The latest major modification was carried out by the TecNetwork project in 2019 and was part funded by Business Finland Oy. The current version of the PL calculation tool has been released to the project partners. The tool is not sold separately, but it is released to customers in assisgnment projects.

The PL calculation tool is mainly targeted at the functional safety experts responsible for calculating PL in the early phases of design. The tool helps to partition PL requirements for subsystems. It can also be used for validation in later design phases.

The PL calculation tool calculates the PL (Performance Level) of safety functions according to standard ISO 13849-1 principles by applying Excel sheets. Excel is a convenient tool for calculation as large tables of component values are used in the calculation and the input and output can be copied from/to other tools. The calculation mainly utilizes $MTTF_D$ (Mean Time To Dangerous Failure) values, DC (Diagnostic Coverage), and the architecture of the safety function circuits. The standard ISO 13849-1 provides calculated tables for PL estimation and these values are applied in the PL calculation tool. The tables are calculated by applying Markov models. The approach of the PL calculation tool supports finding limit values for new components and comparison of subsystems.

The SISTEMA tool (developed by the IFA) has been applied in testing the results, and it is recommended to also test critical parts with SISTEMA. SISTEMA calculates the results by applying analytical equations and the results may therefore differ from the PL Calculation tool. The PL calculation tool also provides SIL calculation according to IEC 62061 and IEC 61508-6. The PL Calculation tool provides pre-set parameters from the PL calculation, so parameters do not need to be re-entered for each calculation, and the results of calculations using the pre-set parameters can be read immediately. The parameters can also be replaced with more accurate ones.

Figure 39 shows the structure of the PL Calculation tool. The lines show how it is intended to move from one calculation sheet to another by applying hyperlinks.

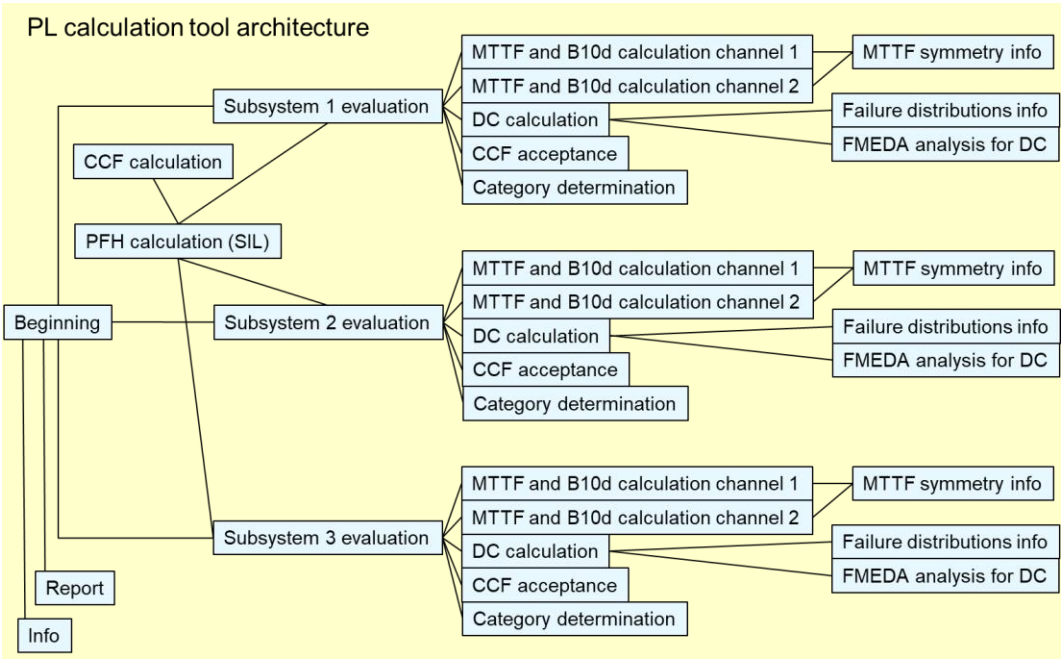


Figure 39. Structure of the PL Calculation tool.

During 2019 new features have been added to the calculation tool, such as FMEDA analysis for DC and SFF (safe failure fraction), SIL (Safety Integrity Level) calculation according to IEC 62061 and IEC 61508-6, and a reporting platform.

FMEDA provides a more accurate result for DC calculation compared, for example, to the tables of ISO 13849-1. FMEDA calculation is based on the following definition of DC: detected dangerous failures divided by all dangerous failures. FMEDA can also be applied for FMEA (Failure Mode and Effects analysis) to find critical failures of the system. In some cases, SFF is also needed and the result can be achieved at the same calculation table as the DC result.

SIL calculation can be applied to verify the PL calculation results. Both calculations use similar analytical equations, but with slightly different parameters. However, some differences are to be expected due to the different calculation. The reporting platform is added to the PL Calculation tool, first to validate the calculation and secondly to report the calculation. The reporting shows the applied calculation structure, which should be the same as the safety block diagram of the safety function. There may be differences due to simplification of the calculation model. The reporting also shows all of the applied components, except those that are calculated as subsystems.

4.3 Fighting a Li-Ion battery fire in underground conditions

Battery powered electrical drives are nowadays also designed for underground mining applications. Electrical drives produce less air pollution and therefore decrease the ventilation power consumption in the mine. In addition, electricity is a considerably cheaper 'fuel' for mining machinery, and electrical machines are considered more reliable than diesel-powered machines due to their simpler structure and fewer parts.
Lithium-ion based rechargeable batteries are also commonly used in heavy work machine applications. They are relatively safe, as there is no primary lithium (lithium metal) present in the battery structure. Lithium oxides, which are not flammable, are used as cathode materials (e.g. LiCoO2). However, Li-Ion cells still contain flammable parts: the electrolyte consists of lithium salt (e.g. LiPF6) which is dissolved to an organic solvent such as methylcarbonate or diethylcarbonate. The anodes are most commonly made of carbon-based, inflammable materials[40]. The separator, which prevents anode-cathode contact but allows Li-ions to pass though, is usually made of plastic (polyethylene (PE) or polypropylene (PP)), which is also a combustible material.

Today, the majority of heavy-duty work machine Li-ion battery cells contain a lithium titanate (LTO) anode. LTO anode cells are inherently safer than other Li-ion battery types as the anode is carbon-free and will not generate metallic lithium, even when the state of charge (SOC) is below the specified level.

Li-ion batteries can reach a self-heating stage that can lead to thermal runaway. All of the components needed for fire are present in the Li-ion cell: fuel, heat and oxygen. Some of the key factors and conditions leading to thermal runaway are presented in Figure 40.

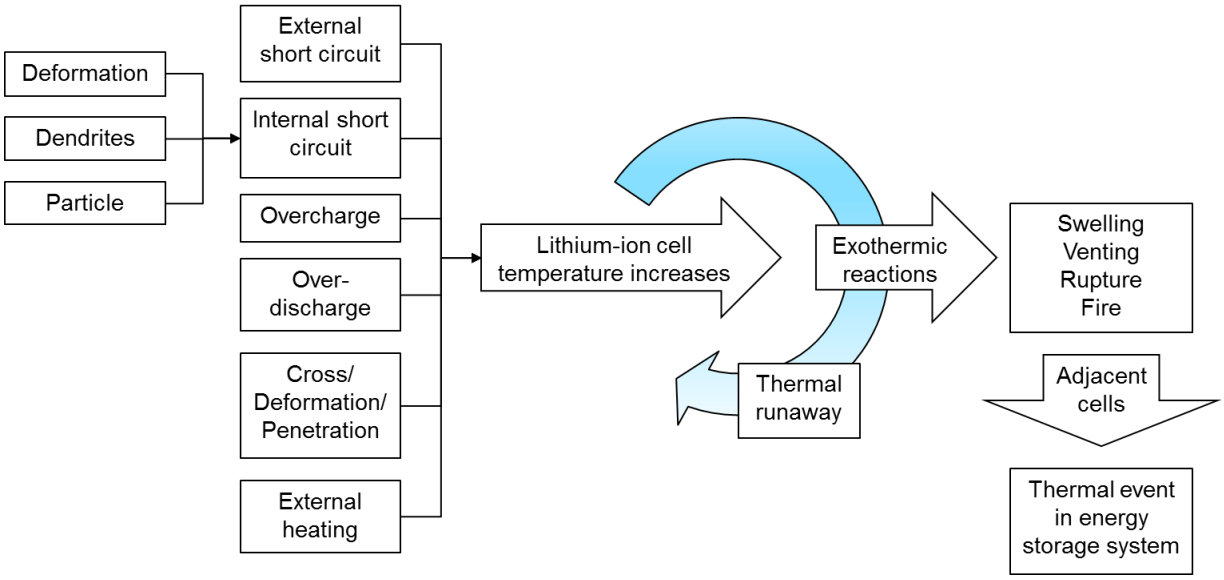


Figure 40. Potential chain of events from Li-ion cell level to energy storage system level.[41]

[40] Lisbona, D. & Snee, T. 2011. A review of hazards associated with primary lithium and lithium-ion batteries. Process Safety and Environmental Protection 89. pp. 434–442. Elsevier.
[41] Adapted from: Andersson et.al. 2017. Safe introduction of battery propulsion at sea. SP Rapport 2017:34. RISE Research Institutes of Sweden. ISSN: 0284-5172. Available at: https://www.diva-portal.org/smash/get/diva2:1118026/FULLTEXT01.pdf

Thermal runaway and heat effects in lithium-ion cells are sensitive to the state of charge (the higher the charge voltage the lower the onset temperature) and depend on the history of the cell and the load applied.

There are several control mechanisms for protecting Li-ion batteries against hazardous effects:

- At the battery hardware level, safety mechanisms involve cell design features such as safety vents, shutdown additives, current cut-off device and separator materials.
- At the system hardware level, electronic control to prevent overcharge, over discharge and overheating of the battery packs is necessary, including balancing to prevent unbalanced states of charge among packs.
- The electrical hardware is essential to providing safety at the system level. Fuses are needed to protect against high current excursions in the system performance, and contactors minimize the possibility of external short-circuit.
- Batteries must be provided with structural protection as well as a thermal management system (e.g. adequate ventilation) to prevent overheating due to operation or heat input from the surroundings. Thermal management of the group of cells forming the pack and module is necessary to prevent propagation of these thermal effects.

Safe operation of battery systems also requires controls at the software system level. Measurement of battery performance is necessary to ensure safe operation. Good indicators of cell performance are battery cell/pack voltage, temperature, current and state of charge.

4.3.1 Combustion behaviour of large-scale lithium-titanate battery

In Hefei, China, a research team tested in 2014 the combustion behaviour of a large-scale lithium battery[42]. Three 50 Ah lithium-titanate batteries were heated with an electric heater until combustion. It was found that when the battery temperature exceeds a certain value, a series of reactions occur:

- breakdown of solid-electrolyte interphase for carbon-based anode,
- melting of separator,
- reaction between the negative material and electrolyte,
- decomposition of electrolyte,
- reaction between positive material and electrolyte etc.

The cathode materials in Li-ion batteries are thermally unstable and release oxygen at elevated temperature, inducing an autocatalytic reaction with the electrolytes. It was also found in the tests that charged batteries are more hazardous than uncharged batteries.

4.3.2 Emissions in battery fire

The Finnish Institute of Occupational Health, FIOH, is a research and specialist organization in the field of occupational health and safety. In 2016, the FIOH conducted a series of fire

[42] Huang, P., Wang, Q, Li, K., Ping, P. & Sun, J. 2014. The combustion behavior of large-scale lithium titanate battery. Scientific Reports 5 : 7788. https://www.nature.com/articles/srep07788

tests with Li-ion battery cells (type 515.1740.A, cathode material NMC)[43]. This battery cell type was formerly used in the Think[44] electric car. The tests were conducted at the Emergency Services College[45] in Kuopio, Finland.

Significant amounts of hazardous gases were produced during the battery fires. The most significant of these were emissions of hydrofluoric and hydrochloric acids. The average concentrations of hydrofluoric and hydrochloric acids measured in the FIOH tests are summarized in Table 5, compared with FIOH and AEGL limit values.

Table 5. Average concentrations of hydrofluoric and hydrochloric acids in air during Li-ion battery fire compared to some limit values.

	hydrofluoric acid (= hydrogen fluoride, HF) concentration (mg/m3)	hydrochloric acid (= hydrogen chloride, HCl) concentration (mg/m3)
Burn 1 (FIOH tests)	9.2	4.3
Burn 2 (FIOH tests)	18.0	3.5
Finnish HTP values (concentration known to be harmful), max. 15 minutes exposure time	2.5	7.6
AEGL 1 (1 h): Notable discomfort, irritation, or certain asymptomatic non-sensory effects.	0.8 (1 ppm)	2.7 (1.8 ppm)
AEGL 2 (30 min): Irreversible or other serious, long-lasting adverse health effects or an impaired ability to escape.	28 (34 ppm)	65 (43 ppm)
AEGL 3 (30 min): Life-threatening health effects or death.	51 (62 ppm)	313 (210 ppm)

4.3.3 Fighting a Li-ion battery fire – best practices

In 2012, the Fire Protection Research Foundation in the US initiated a research programme to develop best practices with firefighting tactics as one of focal areas. One outcome was the research report 'Best practices for emergency response to incidents involving electric vehicle battery hazards: A report on full-scale testing results'[46]. Based on full-scale tests, the following best practices for firefighting tactics and personal protective equipment (PPE) were suggested and observations were made:

[43] The FIOH report is available online (in Finnish only): https://spek.onedu.fi/koulutus/wp-content/uploads/sites/2/2017/12/Loppuraportti-final-1949_001.pdf
[44] Think! electric car: https://en.wikipedia.org/wiki/Think_City
[45] The Emergency Services College: https://www.pelastusopisto.fi/en/
[46] Long, R.T., Blum, A.F., Bress, T.J. and Cotts, B.R.T. 2013. Best practices for emergency response to incidents involving electric vehicles battery hazards: A report on Full-Scale testing results. Fire Protection Research Foundation. URL: https://www.nfpa.org/News-and-Research/Fire-statistics-and-reports/Research-reports/Electrical-safety/Emergency-Response-to-Incident-Involving-Electric-Vehicle-Battery-Hazards

- Similar PPE and fire suppression / extinguishing equipment to that used in conventional vehicle fires are appropriate also for use against fires involving battery-powered vehicles.

- Any individuals without PPE and Self Contained Breathing Apparatus (SCBA) should remain beyond a 50-foot (~15 metre) radius of the fire.

- Due to the longer extinguishing time required than in conventional internal combustible engine (ICE) vehicles, there should be either enough responders on site to enable firefighter rotation or SCBA cylinders should be able to be switched quickly.

- Use of water does not present an electrical hazard to firefighting personnel. The current PPE is appropriate also with regard to electric shock hazards during non-invasive suppression operations (cutting, piercing etc. operations not included), as during the full-scale tests no significant current or voltage readings were indicated in any of the suppression tests.

- Water without any additional additives was able to suppress the fire in every test. The required amount of water increased as the total battery size increased or when the battery was less accessible due to vehicle layout (e.g. protective battery case). Continuous water flow directly on the battery can shorten time to full extinguishment, but the total amount of water could increase.

- First responders should prepare to suppress the fire at least for an hour or more. In one test the battery reignited 22 hours after the fire was first extinguished. Thermal imaging can be used to monitor the battery cooling process, but it can also provide false security, because the vehicle components and structures and the outer shell of the battery can prevent reliable measurements.

- Damaged or burned Li-ion battery should be stored more than 50 feet from any combustible materials until the battery can be safely discharged.

- If a suitable water source is not accessible and there are no threats to life safety or to nearby combustibles, allowing the battery pack to burn to extinguishment may be a viable alternative to suppression. In the tests, the battery pack burned with visible flame for approx. 90 minutes.

If only pure water is used as a suppression agent, the disposed water will not be heavily contaminated; it is slightly more acidic and contains some chloride and fluoride. No special treatment of spent fire suppression water is required.

4.3.4 Suppression of Li-Ion battery fire

Large amounts of pure water or water-based extinguishing foam are generally recommended for suppressing a lithium-ion battery fire. Use of water mist as an extinguishing agent is said to promote the formation of unwanted gases, and in tests conducted in Sweden[47] limited measurements showed an increase in hydrogen fluoride (HF) production rate during the application of water mist, although no significant difference in total HF emission levels was detected with or without the use of water mist.

German company Ellermann Eurocon has developed a container called ‘Red Boxx’ for extinguishing electric car fires[48]. In Ellermann’s solution the entire car is moved into the

[47] Larsson, F. et.al. 2017. Toxic fluoride gas emissions from lithium-ion battery fires. Scientific Reports volume 7, Article number: 10018. https://www.nature.com/articles/s41598-017-09784-z

[48] https://ecomento.de/2017/02/10/dieser-loesch-container-fuer-brennende-elektroautos-macht-es-der-feuerwehr-einfacher/

waterproof container and submerged in water to ensure constant cooling and prevent reignition. Work machine batteries can weigh several tonnes and surface cooling alone may therefore be ineffective. Submerging an entire work machine in water is, however, not possible in practice in the vast majority of locations. Battery packs should therefore be designed to enable only the overheated battery pack to be cooled, preferably by utilizing the existing cooling channels used for battery pack temperature management. A waterproof outer structure would also provide protection against physical stresses from the environment such as falling rocks or collisions with tunnel walls, etc. Container-like battery pack protection significantly decreases the amount of extinguishing or cooling water required and provides an effective way to extinguish and cool an overheated battery without risk of re-ignition.

In the battery combustion tests conducted in the US, samples of the suppression water were collected and sent for laboratory tests. The water sample exhibited a slightly lower pH value than the control sample collected from the suppression water source. Low levels of chloride and fluoride anions were also detected. The presence of hydrogen cations increases the acidity of the solution, causing the pH to drop. The concentration of chloride in the sample was only 2 to 3 times greater than normal detected levels, but the concentration of fluoride in the solution was more than 100 times greater than normal detected levels. Furthermore, according to the tests conducted in the US, cooling water spray or mist presented no risk of electric shock from the battery.[49]

Aqueous Vermiculite Dispersion (AVD)

Aqueous vermiculite dispersion (AVD) is a fire extinguishing agent suitable for extinguishing small lithium ion battery fires such as mobile phone or laptop computer fires. One supplier website[50] explains the principle of vermiculite extinguisher as follows:

> *'The vermiculite particles within the mist are deposited on the surface of the burning fuel to create a film over the top of the fire. The film instantly dries and because the high aspect ratio platelet particles overlap and bind together, they produce a non-flammable oxygen barrier between the fire and the atmosphere. This process offers a cooling to the surface of the fire and as the AVD platelets begin to build up the layer of vermiculate particles on the top of the fuel source, the fire is gradually cooled and brought under control.'*

AVD extinguishing systems are available in different sizes from small portable extinguishers to modular units for rapid response units. Fixed delivery systems are also available for high risk environments.

F-500 Encapsulator Agent

F-500 Encapsulator Agent (Hazard Control Technologies Inc.) is claimed by the manufacturer to be effective at suppressing lithium-ion battery fires[51]. F-500 reduces the surface tension of water, i.e. reduces the size of water droplets. The small water droplets absorb heat 6-10 times more effectively than pure water and penetrate further into the material on fire. The recommended F-500 concentration in water in the case of lithium-ion battery fire is 3%. According to the materials found on the manufacturer's website[52], Dekra, Daimler and Deutsche ACCUmotive also tested agents on lithium-ion battery fires and

[49] Long, R.T., Blum, A.F., Bress, T.J. and Cotts, B.R.T. 2013. Best practices for emergency response to incidents involving electric vehicles battery hazards: A report on full-scale testing results. Fire Protection Research Foundation. URL: https://www.nfpa.org/News-and-Research/Fire-statistics-and-reports/Research-reports/Electrical-safety/Emergency-Response-to-Incident-Involving-Electric-Vehicle-Battery-Hazards

[50] Dupré Minerals Limited, England: https://www.avdfire.com/.

[51] http://www.hct-world.com/industry-applications/industry/automotive/

[52] http://www.hct-world.com/wp-content/uploads/2013/06/CH_F5_AUT_Chronology-Fire-Suppression-for-Hybrid-and-Electric-Vehicles_V2.pdf

concluded that F-500 EA was the recommended agent for extinguishing hybrid and electric vehicle fires.

Instructions for fire suppression

The battery pack modules used in different machines are often very similar, but the machines themselves can differ in structure considerably depending on the model. To ease the task of first responders, machine type specific instructions should therefore be prepared. The instructions should be based on a structured, analytical approach where the whole scenario from identification of the ignition sources to full suppression are analysed. The instructions should also contain a quick-check guide to help operators identify a battery fire, as not all electric work machine fires are necessarily caused by batteries.

4.4 Safety concepts for autonomous and semi-autonomous mobile work machines

4.4.1 Need for automated mobile work machines

Interest in autonomous mobile work machines is on the increase. This is partly related to the development of autonomous cars, AGVs (Automated Guided Vehicles) and automated mobile work machines in closed environments. However, the current examples only operate well in specific conditions. Sensors operate well only indoors, the safety of outdoor sensors is limited, and safety requirements are ambiguous.

The level of automation affects the safety requirements. The more automated system, the more requirements there are for the system, and the more the manufacturer needs to take responsibility. In manual systems, the operator/driver takes a great share of responsibility for system operations. In many cases, the intention is to increase the level of automation gradually, leading to situations where both manual and automated machines operate at one time. From the safety point of view, this is difficult, since both human errors and machine failures may cause hazardous situations.

Currently safety problems with autonomous outdoor mobile work machines can be tackled by applying a closed automation system (access control) and technology to control access to the system. The following differences can be identified between indoor and outdoor mobile machines:

- Sensors do not yet have adequate or stable detection ranges for demanding outdoor operating environments. It is possible that a well-functioning sensor system will be introduced in the near future.
- The speed of mobile work machines is higher than the speed of indoor machines. There is an increasing need for productivity, and machine speed is one influencing factor.
- Most sensors cannot see behind corners or obstacles. This is a problem for on-board sensors, which would be (otherwise) a good solution for free access areas.
- Access control for outdoors systems can be difficult, since there are seldom natural walls and the area is larger than in indoors systems. Autonomous systems are becoming ever larger and fences are becoming more expensive.

4.4.2 Automation safety requirements

The current standards regarding automation safety define closed and open automated areas. Closed automated areas require access control, but machines within them can drive relatively fast. Open automated areas require mobile machines to carry sensors and their maximum speed is slow (below 1.2 m/s) to enable stopping ahead of potential collisions or

upon hard impact force (via tactile bumpers). All access inside the system must be strictly controlled. Typically, safety devices for human detection need to be compliant with PL d requirements (ISO 13849-1)[53]. Many autonomous machine standards are still in the draft phase, and the existing standards are evolving. The standards are expected to become more precise as we learn more about the performance of autonomous systems. The current standards and standard drafts for common autonomous mobile machines are:

- ISO 17757:2017. Earth-moving machinery and mining — Autonomous and semiautonomous machine system safety.[54]
- ISO/DIS 3691-4:2018 (draft). Industrial trucks — Safety requirements and verification — Driverless trucks.[55]
- ISO/DIS 18497.2: 2016 (draft). Agricultural machinery and tractors — Safety of highly automated agricultural machines — Complementary element. 18 p.[56]
- EN ISO 13482:2014 Robots and robotic devices. Safety requirements for personal care robots.[57]
- ISO/WD 21815-1:2018. Earth-moving machinery -- Collision awareness and avoidance -- Part 1: Performance requirements and tests.[58]

The requirements of the above standards tend to lead towards slow or isolated systems, which are the current state of the art.

4.4.3 Strategies to improve the safety of autonomous systems

Strategies for improving safety consider the relationship between humans, technology and the operating environment[59]. Different strategies can also be applied in different parts of a system or two strategies in one place in order to increase the safety level.
We have divided the safety strategies of autonomous mobile work machine systems into three groups (see Figure 41)[60]:

1. Rules for moving in the restricted area (closed area). Only authorized persons and machines may enter the restricted area, and all authorized persons entering must know the rules for moving within the restricted area. This strategy applies typically to manual systems, and safety is highly dependent on the safety conduct of personnel within the area. The strategy closely resembles road safety rules. Typically, other strategies also need to be applied to reach an adequate safety level with autonomous machine systems.
2. Isolated area. The restricted area is isolated and persons enter through an access control system, which stops the autonomous machines in the area. The restricted area may consist of several areas and autonomous machines are stopped only if a person/manual machine and an autonomous machine are in the same area. A clear benefit of the isolated area strategy is that machines can operate at high speed without compromising safety. The safety level can be adequate for all kinds of autonomous systems.

[53] SFS-EN ISO 13849-1. 2015. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design. Finnish Standards Association SFS. 193 p.
[54] ISO 17757:2017. Earth-moving machinery and mining — Autonomous and semiautonomous machine system safety. 36 p.
[55] ISO/DIS 3691-4:2018. (draft). Industrial trucks — Safety requirements and verification — Part 4: Driverless industrial trucks and their systems. 42 p.
[56] ISO/DIS 18497.2: 2016 (draft). Agricultural machinery and tractors — Safety of highly automated agricultural machines — Complementary element. 18 p.
[57] ISO 13482:2014. Robots and robotic devices — Safety requirements for personal care robots. 79 p.
[58] ISO/WD 21815-1:2018. Earth-moving machinery -- Collision awareness and avoidance -- Part 1: Performance requirements and tests. 45 p.
[59] Tiusanen R., An approach for the assessment of safety risks in automated mobile work-machine systems, VTT Science 69, Doc. thesis, 2014, 200 p. + app. 6 p.
[60] Malm T. & Ahonen T. Safety concepts for autonomous and semi-autonomous mobile work machines. Safety of Industrial Automated Systems 2018, Nancy. pp 103-108. www.inrs-sias2018.fr/upload/Proceedings%20SIAS2018.pdf

3. Safe separation distance. On-board sensors detect people or manual machines in front of or near to autonomous machines. The separation distance can also be controlled via a central control system, which knows in real time the locations of all machines and personnel. This usually requires active tags or transmitters, which send their location to the central system. One advantage of the central system is that personnel and machines can be observed even behind corners and obstacles. The safety level is adequate for indoor systems, but for outdoor solutions additional safety measures are typically required.

The colours in Figure 41 represent the typical safety capability of the safety strategy. Red represents low capability and green high capability. The corners of the triangle represent the three strategies described above. In addition, some safety strategies and concepts are located between the corners.

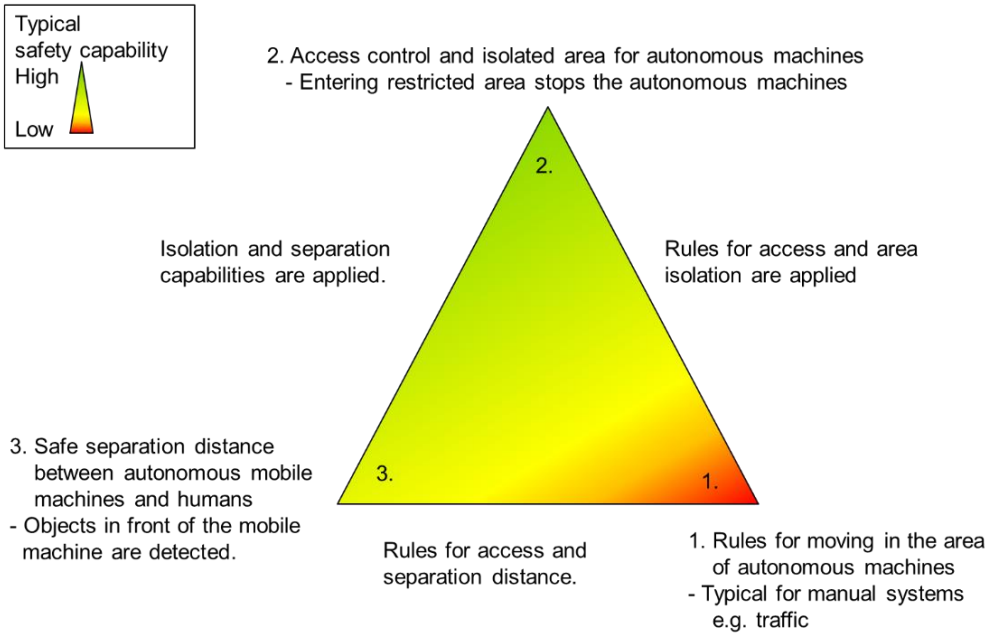


Figure 41. Safety strategies for autonomous mobile work machine systems.[61]

4.4.4 Safety concepts

Safety strategies often lead to the use of specific safety concepts that can be best utilized to improve the safety of the system. Several safety concepts can be applied in one system and strategies can overlap and differ in different parts of the system. Table 6 presents some examples of safety concepts and their associated strategies.

Table 6. Examples of safety concepts and associated strategies.

Safety concept	Rules for automated area	Isolated area	Safe separation distance
Rules for automated area	Rules, devices for better situational awareness, training, semi-automated	Additional means needed for isolation	Additional means needed for detection

[61] Malm T. & Ahonen T. Safety concepts for autonomous and semi-autonomous mobile work machines. Safety of Industrial Automated Systems 2018, Nancy. pp 103-108. www.inrs-sias2018.fr/upload/Proceedings%20SIAS2018.pdf

Safety concept	Rules for automated area	Isolated area	Safe separation distance
	operations under supervision, hold-to-run devices, traffic lights		
Remote control	Rules for applying remote control	Human supervision for e.g. access to another area or handling of objects in delicate conditions	Camera control/supervision, line of sight control, alarms, hold-to-run-devices, detection of correct load handling
On-board safety system	Specific lanes for machines and persons, access for trained personnel	Safety level optimization and protective actions according to the area, lines of defence approach	Limited speed, stopping and rerouting, radar, lidar, proximity sensors, safety bumpers
Centralized positioning system	Actions can be predesigned and optimized for machines	Central system can occupy areas in advance and optimize speed of the machines	Central system optimizes routes, speed and separation distances of machines, can detect objects also behind corners and obstacles, only tagged persons allowed to enter the area, UWB, RFID
Isolated area	Rules for persons allowed to enter the restricted area.	Access control, stop the system when a person or a manual machine enters the restricted area, fences, light curtains	Areas can be occupied to match the separation distance, safety level optimization, lines of defence approach.

Rules for automated areas

The strategy of rules aims at achieving safety primarily by increasing the situational awareness of personnel and by providing rules and guidelines for operating within the automated area. According to the Machinery Directive[62], machine safety design must follow three steps, in order: 1) Inherently safe design, 2) Protective measures, 3) Inform users. The two first steps may not be neglected. Additional means are often required to ensure safety. Similar to normal traffic rules, safety depends on all personnel understanding and observing the ‘rules of the road’. Violation of the rules, such as keeping to lanes, can cause a serious hazard, especially if lanes or the safety distance between lanes are too narrow to allow evasive action.

On-board safety systems

On-board safety systems refer here to safety systems that rely on sensors and devices mounted on the machine (see Figure 2). Detection of an object may trigger speed reduction, stoppage, or rerouting to avoid collision. Typical sensors applied in this approach are: lidar, laser scanner, radar, UWB, 3D-camera, IR camera, proximity detectors (ultrasonic, optical, capacitive) and tactile bumpers. Sensor fusion can also be applied to compensate for the shortcomings of different sensor types. This concept is used, for example, to detect objects

[62] Machinery Directive 2006/42/EC. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). 63 p.

behind corners or small objects next to large objects. For most of the above-mentioned technologies it is difficult to detect a person beside a wall (or other large object). If the machine and large object position were accurately known, it would be possible to adjust the detection range to be close to the wall, although not in all circumstances. In favourable conditions, active tags can be detected also behind objects, but this, too, is highly situation-dependent. In addition, dead battery prevention, faulty transmitter detection, and the need for system redundancy need to be considered.

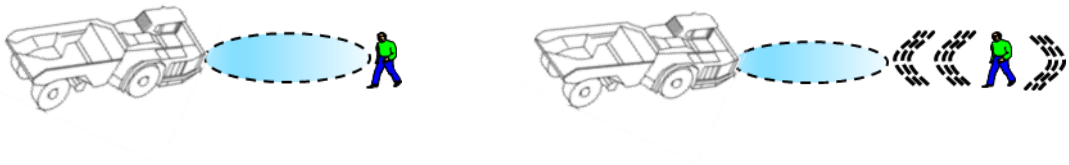


Figure 42. Left: On-board safety system on an autonomous mobile work machine. Right: Detector on each autonomous mobile work machine and active tags on each moving object. (Figure: dumper hauler[63]).

Centralized systems

A centralized safety system functions as part of the fleet management system. It continuously monitors and controls the precise location of all tagged vehicles and persons on the site (see Figure 43.). Each object on site is equipped with its own location system that informs the central system of its position. Usually, several different systems are applied to ensure the position information and to improve accuracy. Continuous communication enables objects behind corners or obstacles also to be detected. Fleet management can also control crossings by controlling speeds and rerouting automated machines to avoid collisions. Typical technologies for positioning objects are: UWB, GPS, IMS (inertia measurement system), odometer and optical measurement systems.

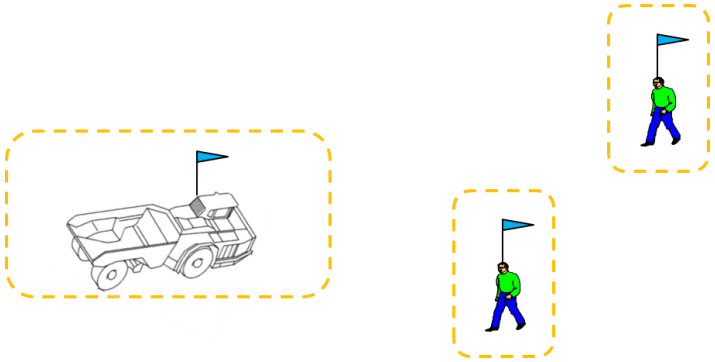


Figure 43. Each moving object sends its position to the central control unit. (Figure: dumper hauler[64]).

Isolated area

The safety system controls and monitors access to each area of the site and assigns persons and mobile machines to specific sectors (see Figure 44). If a person enters an occupied area, then all machines in the area stop. If a machine drives to the boundary of, or enters, an occupied area, it stops. This ensures adequate separation distances between objects. The isolation can be implemented using fences and gates or light curtains (or other

[63] ISO/DIS 19296.2:2015. Mining and earthmoving machinery — Mobile machines working underground — Machine Safety. 47 p.
[64] ISO/DIS 19296.2:2015.

contactless sensors). Gates can be used to prevent access to occupied areas and to provide personnel with safe access beside the occupied area.

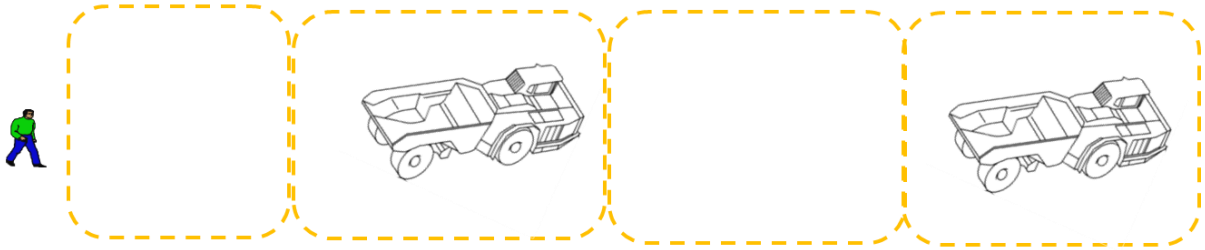


Figure 44. The restricted area for autonomous mobile work machines is divided into separate sectors, each assigned to a specific object. (Figure: dumper hauler[65]).

4.4.5 Discussion concerning safety concepts

With current technology, isolation is the clearest means of ensuring the safety of an autonomous mobile work machine system. For relatively small systems, machine area isolation is a practical way of achieving adequate safety. In large open systems, however, barriers become unfeasible due to the length of barrier required. Isolation is therefore not a sufficiently scalable strategy and can become expensive.

Applying rules to an autonomous system is a scalable and economical strategy, but the safety of rules-based solutions is considered relatively low. The strategy entails some investment costs in the form of traffic lights, traffic signs and road markings, as needed, as well as personnel training.

The safe separation distance strategy has a clear technological orientation, as the distance between personnel and moving machines must be measured. Currently, all sensors have certain weaknesses depending on the operating conditions or environment; however, sensor technologies are improving constantly and prices are coming down. Sensor fusion can also tackle some weaknesses of individual sensors. Indoor safety can be usually addressed by applying low speed limits and appropriate safety sensors. Outdoor safety is more problematic, as sensors are less reliable in rain, fog or muddy conditions and longer driving distances require relatively high speeds (manual driving vs. automated driving speed). The separation distance strategy is to some extent scalable, but each object in the area requires technology, which raises the costs. Outdoor safety strategies are thus much more exposed to demanding operating and environmental conditions.

In all of the three strategies, a challenge is how to deal with uncertainty. In the ‘rules’ strategy it is uncertain whether all personnel will obey the rules. In the ‘separation distance’ strategy sensor performance in outdoor applications is unreliable and highly dependent on environmental conditions. In the ‘isolation’ strategy the means of isolation may vary. Locked doors and high fences guarantee good isolation, but there are situations when people need to enter the area. Complete isolation is not practical. Keys or rules for entering the system can be applied, but then also uncertainty increases. Designers of autonomous mobile machine systems need to accept some degree of uncertainty, but the risks must be well controlled. Currently, there are very few good examples of safe and practical autonomous mobile machine systems. More examples are needed, and the standards also need to evolve in order to define more clearly the acceptable levels of uncertainty and risk.

[65] ISO/DIS 19296.2:2015. Mining and earthmoving machinery — Mobile machines working underground — Machine Safety. 47 p.

5. Development of services in a business ecosystem

Drivers for networked service development

There is an identified need for a transition from transaction and sub-contracting based collaboration models towards more integrated practices in company ecosystems. Customers are expecting more holistic service offerings and, as the complexity increases, companies are not able to hold all the required expertise and knowledge in-house. For individual companies, new collaboration models may provide new business opportunities and growth potential. This relies on the active role of the service integrator but also calls for transparent and active information exchange across the whole network.

A continuous joint innovation process within the network is needed that emphasizes the role of customer understanding. Thus, joint efforts towards full-line service offering development should be based on a profound understanding of customers' needs. The top three development areas specifically requiring collaborative actions are:

- IoT and digitalization with real-time analysis and control, enabled by sensors connecting assets, information architecture built for connection, and smart domain-knowledge driven analytics
- Electrification in mining assets and steps towards 100% electric mining operations
- Increase in automation and steps towards autonomous operations

Experiences of collaborative development

There is a mutual interest in collaborative asset management service development among system and component manufacturers. Collaborative development and effective utilization of each other's existing capabilities seems beneficial for both system and component providers. However, more holistic services provided in a business network necessitates new understanding of how lifecycle costs and profits are managed and value can be created. Provision of new technologies, adaptation of novel business models, definition of new roles in the network, and creation of new processes for the provision and management of the services require tools for managing the risks and opportunities.

There is a clear need for effectively integrating companies' offerings to meet the customers' needs. Thus, there is a demand for integration and coordination during the innovation process and in customer collaboration. According to Valjakka and Valkokari (2015)[66], the service integration tasks are:

1. Defining services through interactions in the complex B2B service network
2. Successfully linking the various resources
3. Supporting value co-creation between the parties involved.

According to the experiences gained in the TecNetwork project, collaborative development calls for management of the following key aspects:

- Openness and transparency: There is willingness to move from transaction-based business models towards more integrated partnerships with increased collaboration. This also changes the way organizations should share information on their strategies and development roadmaps. A more transparent approach is thus required. For

[66] Valjakka, T. & Valkokari, K. 2015. Service network integration - a case study in manufacturing maintenance services. International Journal of Services Sciences 5(3/4):182.

OEMs, the transformation from earlier product development practices in which information sharing was tightly limited until product launch towards collaborative and transparent practices has been on-going for years. Making use of the opportunities offered by digitalization requires collaboration, starting from the strategic level.

- Exchange of information and knowledge: A variety of methods, tools and platforms exist for the exchange of information in a business network and in the product design process. However, the most important factor here is mutual understanding of the targets of the whole network and thus the commitment of companies to required openness.
- Customer orientation: Ecosystem members should have a mutual understanding of the vision, objectives and the ways to achieve the desired results. Therefore, a roadmap that helps to understand the business environment and customer needs and integrates companies' current and future offerings should be created together. A thorough understanding of the strategic objectives of potential customers needs to be formulated. Only then can the technological implications be analysed and discussed by the whole ecosystem.
- Roles and operational practices: The integrator role needs to be emphasized, particularly in the creation of new customer knowledge and in the integration of service offerings. In the development of a new ecosystem, facilitation of the work is needed, particularly in relation to the collection and sharing of customer needs, formulation of the preliminary offering, idea sharing, and R&D and customer work.

5.1 Data-based services

McKinsey & Company (2015)[67] identified the following value creation potential for digitalization in mining:

a) Deep understanding of the resource base
b) Optimization of material and equipment flow
c) Improved anticipation of failures
d) Increased mechanization through automation, and
e) Monitoring of real-time performance vs. plan.

Asset management provides a framework that can also be utilized in the identification of value creation potential. ISO 55000[68] defines asset management as activities that support the realization of value while balancing financial, environmental and social costs, risks, quality of service, and performance related to assets.

Digitalization is expected to radically change the success factors of industrial companies (Lee et al. 2015[1], WEF 2014[2]). It is expected to bring changes to productivity, management models and business models. Performance-based contracts have been gaining increasing attention (e.g. https://www.kalmarglobal.com/news--insights/2019/20190625_kalmar-offers-performance-based-contracts-for-oneterminal-customers/). Asset management as a framework can help to understand how the value related to digitalization is created and thus help develop the services enabled by digitalization.

[67] Durrant-Whyte, H. Geraghty, R. Pujol, F. & Sellschop, R. 2015. McKinsey & Company Metals & Mining November 2015. How digital innovation can improve mining productivity. Available at: https://www.mckinsey.com/~/media/McKinsey/Industries/Chemicals/Our%20Insights/How%20digital%20innovation%20can%20improve%20mining%20productivity/How_digital_innovation_can_improve_mining_productivity.ashx

[68] ISO 55000:2014. Asset management — Overview, principles and terminology.

Recently, many industrial companies have approached digital asset management services by developing individual technology solutions and through quick experiments. Quick experiments and the development paths related to different technology areas (e.g. diagnostics, remote monitoring, condition monitoring and data visualizations) have provided a starting point for the development but have not enabled significant business potential or changes in working practices.

While lots of opportunities are seen in the area of predictive maintenance, solutions for mobile working machines and for underground mining are still limited and the development of different use patterns and environments is proving to be very challenging. However, there is still lots of potential for cost savings and innovation potential related to the efficiency of working processes, energy consumption, and lifecycle costs and profits in general. In order to realize the full potential, companies need to challenge the recent operational practices in their organization.

The development of data-based services has been on-going for a long time; however, a focal problem has been that services have been developed as products, without sufficient customer integration. Furthermore, integration of the services to the customers' business has been limited as the decision-making processes (and related information needs) have not been thoroughly understood and considered. Even the forerunners have lots of potential to develop their use of data in all three main areas of asset management: performance optimization, maintenance, and investment management. Information needs and requirements are different at the strategic, tactical and operational levels; however, many IoT solutions mainly address the operational level and there is still much room for holistic development considering all of these levels. This calls for integration of domain knowledge, technological knowledge and strategic thinking in the network.

Table 7 presents the key needs in three topical service potential areas in modern mining environments.

Table 7. Potential for AI-supported asset management services in underground mining.

Operations management & problem solving in a mining environment	Customers in the mining sector are increasingly expecting digital solutions to result in real-time visibility of the entire mine. OEMs and service providers also expect rapid responses to their expressed needs for data-driven solutions. Automated work status and supporting information from assets and work phases enable effective operations management. All relevant information needs to be shared, which is enabled by intelligent assets, information management, analytics, and developed application layers, with mobile and desktop applications developed according to specific needs. Furthermore, two-way (worker-management) information exchange is needed.
Fleet management & maintenance optimization	Customers need a hierarchic approach to fleet data management where support is provided at the company, production systems, automation systems and asset levels. Cumulative knowledge of fleet performance needs to be exploited more (asset owner view vs. OEM view) for the benefit of individual customers. This calls for metrics defined for fleet performance and data collection carried out according to categorization of environments and conditions. Maintenance performance optimization should utilize novel analytics; however, data exploitation should address all maintenance strategies

	and allocation of resources should be based on business-driven, criticality-based maintenance planning.
Periodic reporting & performance monitoring	Manual work for reporting should be minimized; thus, automated reporting at machine, system and production system levels should be put in place. Performance should be monitored in a hierarchical manner, where top-level reporting allows more detailed analyses related to finding root causes of potential problems, failures or bottlenecks, or identification of development targets. Areas for development include the availability performance of the assets at different levels, time and resource efficiency of the system, and operator output quality improvement. OEMs are expected to provide information on the performance of assets, which is further integrated in the mining company's own information system. Thus, provision of performance benchmarking information is expected. From the customers, willingness to share data regarding production and maintenance is regarded as the enabler of benchmarking services.

The use and value of predictive analytics need to be understood in a wider value context, as depicted in Figure 45 (adapted from Ahonen 2019). The framework includes three focal topics of engineering asset management, namely maintenance, operations and investment decision-making, and also highlights the importance of service-product development collaboration and information exchange with effective data utilization.

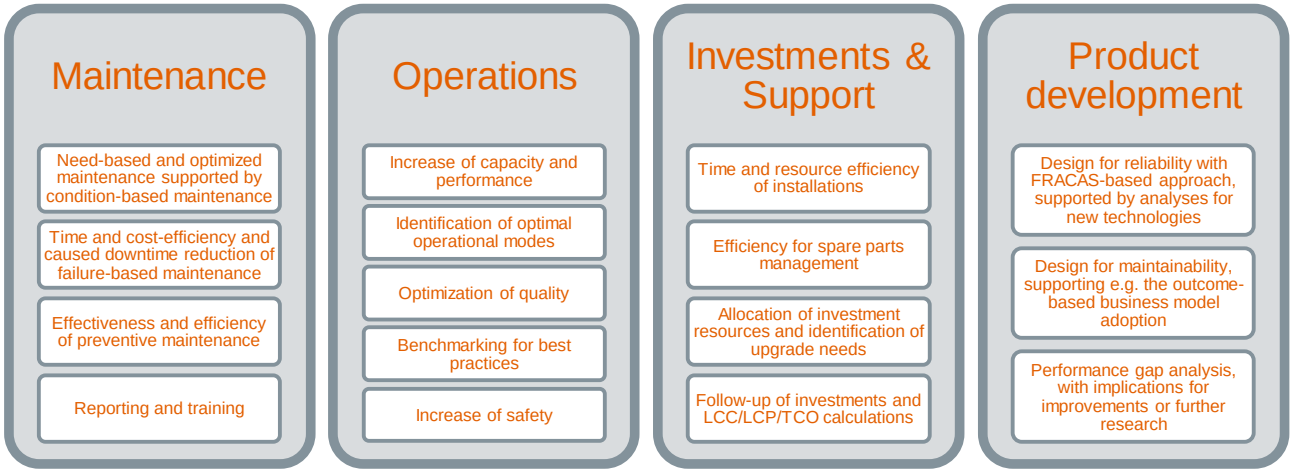


Figure 45. Exploitation of data sources for asset management service and product development purposes (adapted from Ahonen 2019[69]).

Figure 46 presents an example of asset management service offering items. The service offering has been categorized in four categories: fleet management, O&M reporting, performance monitoring and optimization and problem solving. Exploitation of data may also be analysed from the perspective of machine level, process level and fleet level challenges and questions. Furthermore, the questions can also be divided into strategic, tactical and operational levels. In the TecNetwork project, the following considerations have been identified for the above-mentioned levels:

[69] Ahonen, T. Value of predictive analytics in networked asset management service offering. 2019 World Congress Resilience, Reliability and Asset Management. Conference Proceedings. Available at: http://resilienceconference.ethz.ch/

- Machine level: Identification of potential problems by use pattern and overload recognition, predictive models for failure behaviour, component-specific condition monitoring applications, energy usage monitoring and optimization for electric fleets with operator patterns considered.
- Process level: Operator-specific efficiency monitoring and efficiency guarantee as a service (data gathering, analytics, monitoring and recommendations), optimization of the process by minimizing human factors, identifying bottlenecks and ensuring information exchange throughout the process phases
- Fleet level: OEE optimization of processes and availability-driven optimization of assets based on data gathered from a large fleet of assets, with conditions and environments taken into consideration.

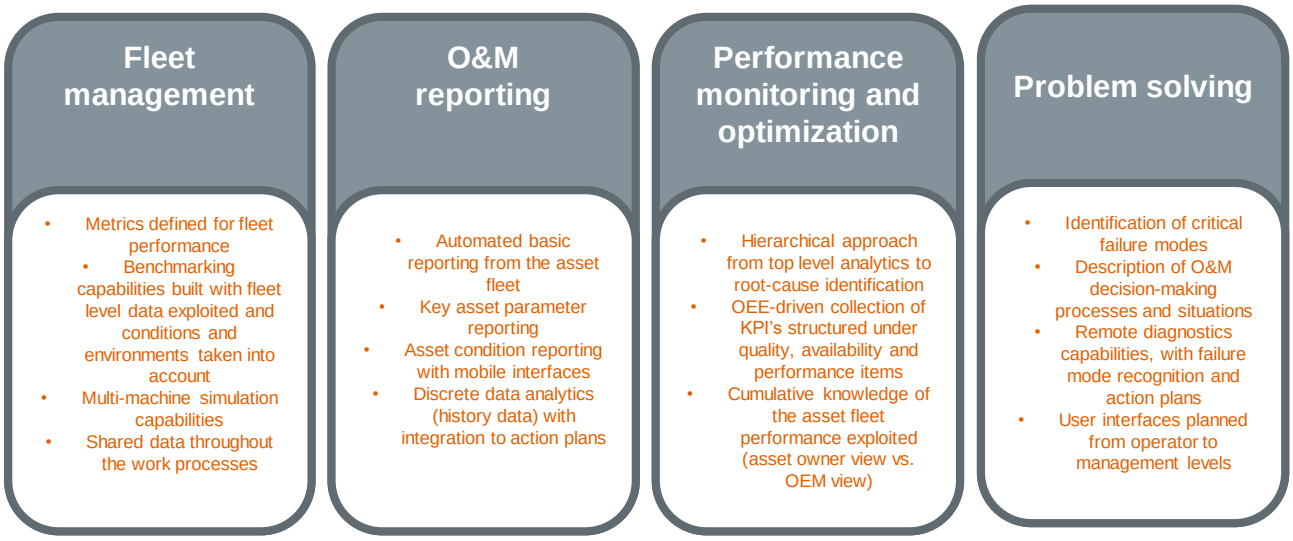


Figure 46. Categorization of asset management services and considerations in underground mining context (adapted from Ahonen 2019[70]).

5.2 Tool for service offering value assessment

Assessing the mechanisms of how services affect customers' operations and business processes requires comprehensive understanding of customers' business in practice. For a value assessment approach adopted in the TecNetwork project (based on results from the previous project Fleet Asset Management, http://virtual.vtt.fi/virtual/proj3/FleetAM/), information on both operational costs and costs related to occurred challenges is required. Assessment of the value elements provides information on which areas the provided services should specifically put focus on. Thus, the value potential of provided services is dependent on the customers' operational and unavailability-based costs. These costs can be reduced by the provided services. Customer needs may vary greatly according to the customer cluster and each customer typically has its own specific needs. It is assumed that the value elements identified are shared for the most part; however, the weights of each element may vary according to the nature of the customer's business.

[70] Ahonen, T. Value of predictive analytics in networked asset management service offering. 2019 World Congress Resilience, Reliability and Asset Management. Conference Proceedings. Available at: http://resilienceconference.ethz.ch/

5.2.1 Analysis of failure modes and bottlenecks and their relation to the service concepts

The operational costs of the customer are evaluated to gain an understanding of the actual value of the savings that could be potentially gained by the services (=value potential). Similarly, analysis of the challenges (failure modes, other types of technical or operational difficulties) offers a structured way of providing information on a) which type of challenges typically occur in each customer cluster, b) what are their effects on the customer's business, c) which challenges are most significant, d) which challenges offer the best potential for the services provided.

Challenges analysis includes the following two steps:

- Firstly, evaluate the 'unit cost' of each potential consequence type, e.g. a 'one hour delay'. These information items are then used when analysing all of the identified failure modes and challenges.
- Secondly, identify the failure modes and challenges and evaluate their consequences, i.e. effects on the customer's business.

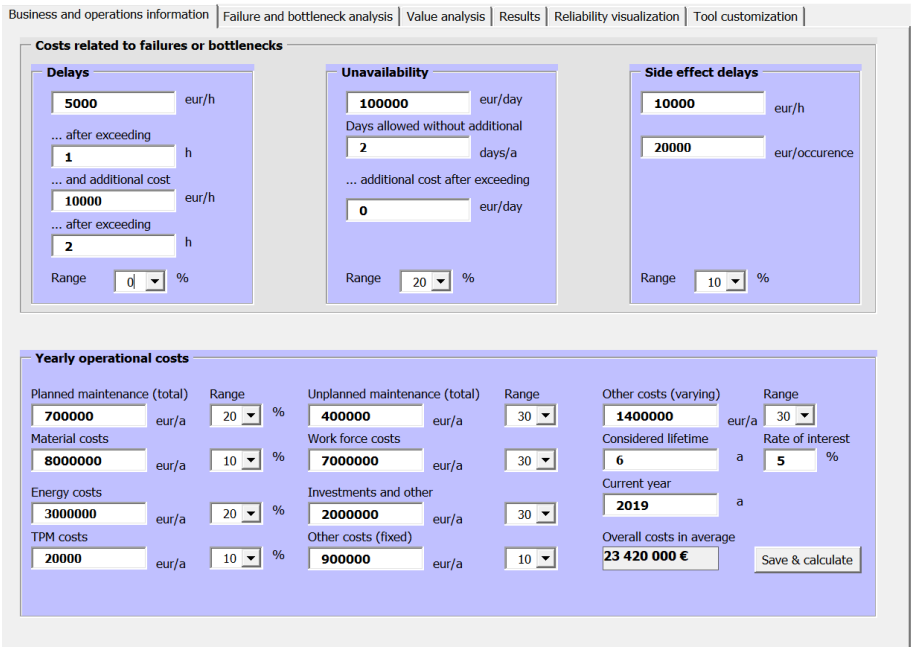


Figure 47. Business and operations information

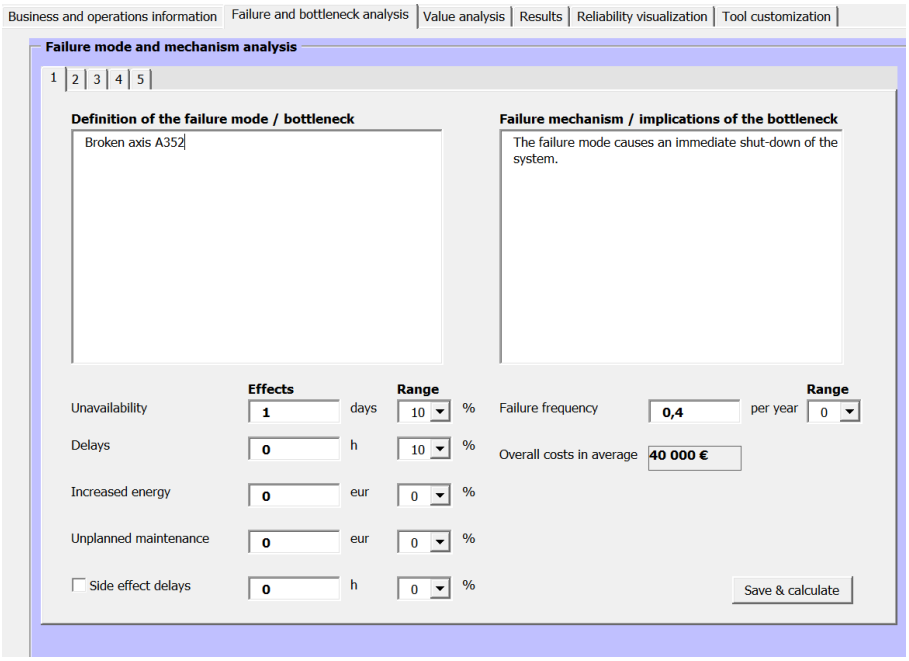


Figure 48. Failure mode and mechanism analysis.

5.2.2 Value analysis

The Value Analysis part of the approach includes assessment of the effects that the considered services have on the customer's cost elements. These cost elements are evaluated according to the main categorization into operational and challenge related costs and the lower level cost categorization utilized in the earlier phase of the analysis. Taking into account all of the considered cost elements, the analysis results in estimations of the cost reductions generated by the considered service(s).

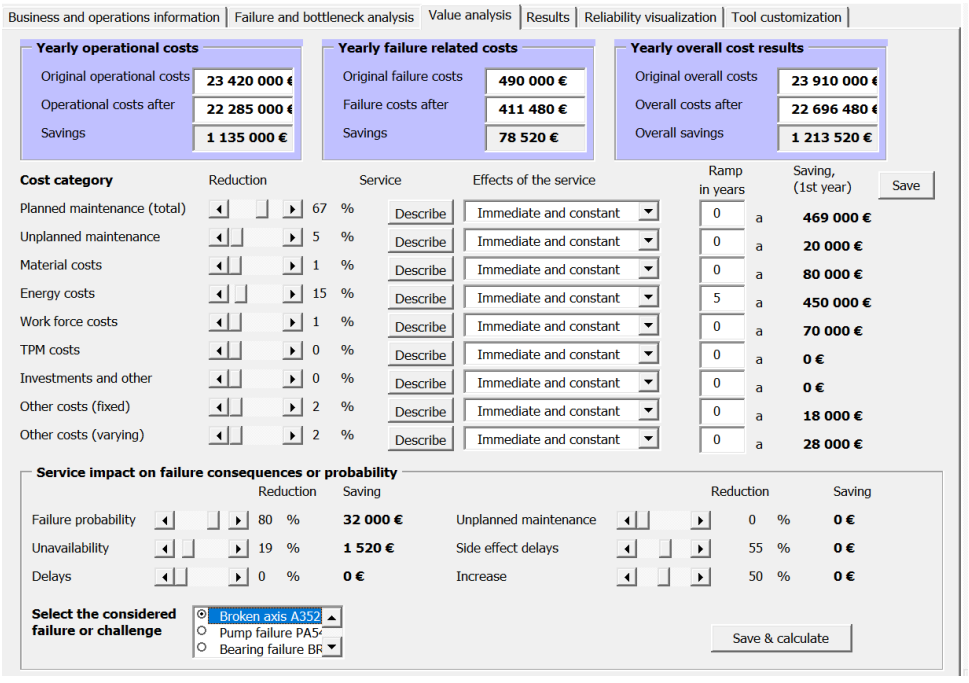


Figure 49. Value assessment.

5.2.3 Use scenarios

The tool modified (from the lifecycle cost and profit related results of the Fleet asset management project) in the TecNetwork project can be utilized for the following purposes or in the following phases when developing and offering services:

- The target price or cost price is known for a service and we want to see how valuable the service must at least be for the customer in terms of money and regarding each significant cost category
    - The profitability of the service is evaluated by estimating whether the service can result in the savings required in order to meet the cost price. From this, we can see whether the service has pay back potential.
    - From this, we can then determine the minimum requirements for the services (for each cost category)
- The content of the services has been outlined and we need to more accurately estimate the real customer value and provide the service pricing activity with supporting information
    - The benefits of the service are evaluated according to each cost category, giving the economic value for the customer
    - By comparing the target price and estimated customer value we can see the real potential of the service (baseline for pricing)
    - If the assessment clearly indicates a lack of customer value related to the addressed cost categories, possibilities for complementing the service portfolio can be considered

The service offering should always be based on the best understanding of what customers are willing to buy (customer value) and tools are needed to show the added value in customer negotiations. The SBVA tool can be utilized both when developing services at the customer cluster level (service development processes) or when wishing to assess customer value for a specific customer (marketing and selling processes). The assessment of customer value and the development of service content can be performed side by side so that, based on the assessments, one can decide on how the considered service should be further developed to reach the required level of added value. Common practices for the assessment of service value and consideration of the specific features of customers' business, as well as for argumentation of the practical benefits of services in the selling processes should be provided. Guarantees of customer value can seldom be provided based on assessments made with insufficient information. Reference cases can, however, be utilized in service selling processes. Alternatively, the service provider and customer can reach a common view on the added value by analysing the value together in a systematic fashion. Close collaboration with the customer during the process and taking customer-specific information into consideration are important as customers emphasize the value elements related to services differently.

6. Electric fleets

Electric mobility is a major trend in practically all segments, and the main driver is the growing concern about ongoing climate change. Electric vehicles are locally emission free, have lower energy consumption than conventional vehicles, and produce less noise. All of these aspects can bring great advantages in underground mines. Electric vehicles are generally more capital intensive than conventional vehicles, but cost savings can be achieved due to their lower operational costs. In underground mines in particular, the costs related to ventilation can be greatly reduced by the introduction of electric vehicles. The design of an electric vehicle system requires a holistic approach, taking into account vehicle design, charging requirements, route network, electric grid limitations, etc. A simulation tool has been developed to support the uptake of electric vehicles. The tool is capable of analysing various vehicle fleets, and both energy consumption and the cost of operation are obtained from the simulations. An optimization algorithm has been implemented using the simulations as a cost function. In addition, a 3D-visualization and route construction methodology has been implemented for mining purposes.

6.1 Trends related to electric fleets in modern underground mines and needs for fleet management

Electric vehicles are increasing in popularity, both when it comes to smaller vehicles and personal cars, as well in the case of heavy-duty vehicles. The driving force for the uptake of electric vehicles is the growing awareness of environmental issues and climate change. For instance, the European clean vehicle directive sets limitations on the minimum amount of required clean vehicles in upcoming public procurements, and 50% of the clean vehicles are required to be fully electric. The required proportion of clean vehicles will increase by 2025. As regards public transport, some cities have even more ambitious targets aiming at 100% zero-emission city buses in about 10 years. While electric city buses are entering full commercial operation, other heavy-duty segments are a few years behind. Nevertheless, the availability of electric alternatives for non-road mobile machinery is steadily growing. The first hybrid vehicles entered the market more than ten years ago, and fully electric vehicles for multiple purposes are already available. The electrification of very heavy vehicles is still a challenge due to the high power and energy need. The largest electric vehicle so far is a 110 tonne electric dumper prototype.

Regardless of the use case and environmental conditions, electric vehicles provide many benefits compared to conventional vehicles, such as lower energy consumption, lower emissions and less noise. However, the operation of electric vehicle fleets differs from conventional fleets due to the limited range of the vehicles. Whereas conventional diesel vehicles are rapidly refuelled, charging of electric vehicles requires much more time. The combination of relatively short range and long charging times makes their operation more demanding and proper planning is required in order to achieve the full potential of electric vehicles.

The general picture of an underground mine is a very unpleasant and dangerous environment with narrow, rough and dark tunnels, poor air quality and high levels of noise. The harsh environment is a challenge for vehicle manufacturers, but locally emission-free electric vehicles have the potential to improve these working conditions and even reduce operational costs due to less need for ventilation power. Mines, both underground and surface, contain hilly routes for transportation vehicles. Driving uphill requires a lot of power, going downhill requires a lot of braking force. In both cases, electric vehicles are beneficial. The efficiency of an electric motor is at its best when the torque and speed are in the vicinity of the rated values, i.e. the motor can be designed for steep inclines. When going downhill,

the same motor can be used for braking and regenerating energy, contrary to diesel-powered vehicles. Electric vehicles are particularly beneficial in cases where the vehicle is loaded going downhill and empty when going uphill, which is a situation sometimes encountered in mines, particularly surface mining. In addition, because the overall efficiency of electric vehicles is higher than diesel-powered vehicles they produce less heat during operation, thus further improving the climatic conditions.

A mining fleet consists of various kinds of vehicles. Some vehicles are used for transport, others are special vehicles used during different phases of the mining process, such as explosive charging, drilling or spraying. Many vehicles are stationary during the actual work phase, and their energy consumption is at its highest during this phase. These machines could be relatively easily replaced with electric vehicles that connect to the grid during the working process, thus eliminating the need for large batteries. Grid-connected vehicles have, in fact, been on the market for quite some time. Furthermore, duty cycles vary a lot from vehicle to vehicle; some vehicles are used almost 24/7, others are used only for short periods at a time with long breaks in between. Battery electric vehicles require frequent charging, and the charging has to be included in the planning of duty cycles. Having a high number of electric vehicles would therefore require charging scheduling to avoid high power peaks. This is particularly relevant in mines, as the grid strength can place limitations on the power availability. The constantly changing route network makes charging scheduling even more challenging.

Safety is always an issue in mines, and this has to be taken into account in the design of mining vehicles. The vehicles have to withstand dust and dirt and mechanical shocks. In the case of electric vehicles, the greatest safety concern is related to the batteries, and battery damage should be avoided in all cases. However, electric vehicles also provide benefits as the automation of these vehicles is much easier than in the case of conventional vehicles. An automated mine is the ultimate goal for mining companies, as it would minimize the need for personnel inside the mine, simultaneously reducing the risks involved. Furthermore, labour costs would be lowered. Fully automatic operation requires, of course, wireless communication and real-time management of the entire fleet.

6.2 Simulation approach for electric fleet optimization, visualization and route optimization, and energy consumption modelling

The transition from conventional diesel vehicles to fully electric vehicles is challenging for a number of reasons affecting practically all kinds of mobility solutions. First of all, battery electric vehicles are characterized by a rather short operation range and limited power, and the vehicles cannot be operated in exactly the same way as conventional vehicles. Secondly, the cost structure of electric vehicles differs from conventional vehicles as their capital costs are relatively high, due largely to their costly batteries. The operation-dependent battery lifetime further complicates the cost analysis. As electric motors are more efficient than diesel engines, energy consumption can be greatly reduced, and operational cost lowered. However, the energy consumption of electric vehicles is highly dependent on the use case, and the variation in energy consumption from case to case is greater than when using conventional vehicles. The required charging infrastructure affects both the operation, i.e. the frequency of charging and time required for charging, as well as the total costs of operation. Planning of the charging infrastructure includes selection of charging locations and charging power as well as the number of chargers. The various needs of all vehicles in the fleet need to be addressed, but ultimately also future needs should be taken into account.

One of the major obstacles in introducing electric vehicles is lack of knowledge and operational data. In order to address these issues, VTT has for several years developed planning tools to assist the introduction of electric mobility. The tool set consists of simulation models including route construction methods for various use cases, cost analysis tools, and power grid analysis capability. Within the TecNetwork project, emphasis has been placed on

the development of tools to tackle more extensive use cases and on offering a real-world show case.

For simulation purposes, a test network based on real plans from the Vuorokkaan kaivos mining network in Otanmäki, Finland, was modelled in 3D. A specific data structure based on enhanced Openstreetmap XML data was used to represent the traversable links within the mine and the network was created based on freely available materials from the internet[71]. The whole network (with axes in metres) is visualized in Figure 50.

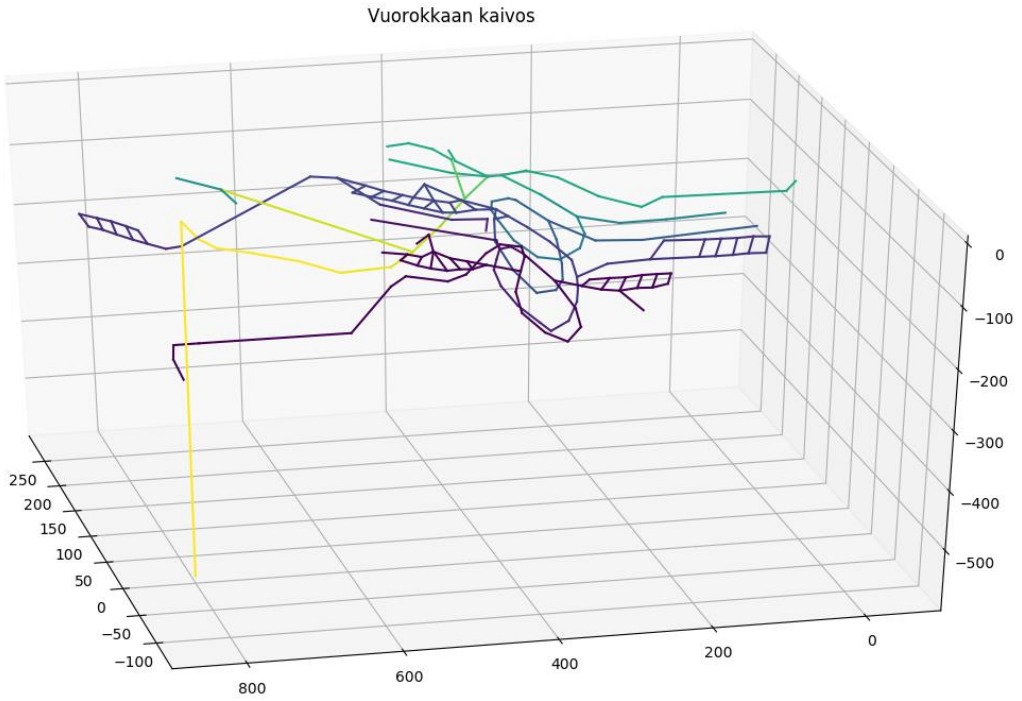


Figure 50. The visualized mining network used for testing. Colours represent the elevation of the highest node of each link.

As the existing mining operation plans for the network were not openly available, an additional tool was developed to assist the creation of the test routes within the duty cycle, although the duty cycle still needs to be created manually. The routing is based on the Dijkstra algorithm and the coordinates have been transformed to standard WGS84 format to maintain compatibility with other simulation types, but the transformation has been simplified for a location of 0° N 0° E. The tool used for the route generation process is shown in Figure 51.

[71] Otanmäki - http://www.otanmaki.fi/Otanmaki_Mine_brochure_2017.pdf - page 10

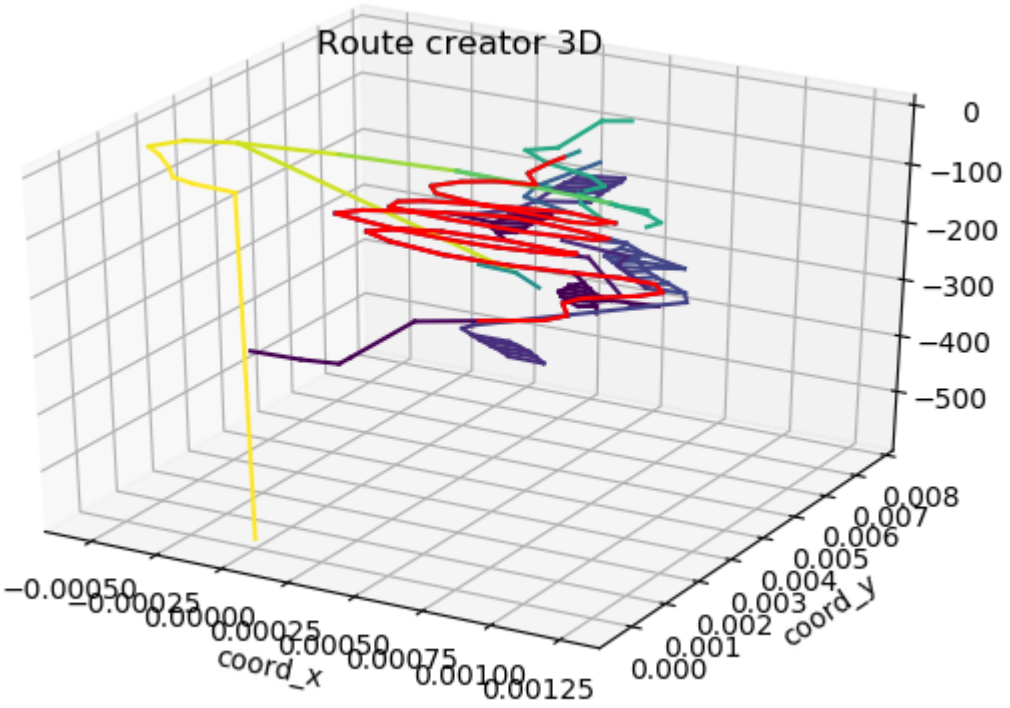


Figure 51. The mining network with a generated connection between two points

The starting point of the simulation model was the single vehicle energy simulation model presented previously[72]. The presented model was constructed primarily for electric city bus simulations where it can be used for evaluating the energy consumption of a selected bus type on a selected route. Hence, the model gives a realistic estimation of the energy consumption of a vehicle given the topology of the route. One major feature is the use of real duty cycles, and the ability to perform simulations without ready-made speed profiles. The model takes into account the location of bus stops and even traffic conditions can be included in order to obtain a realistic speed profile. In addition to city buses, the model can be used for other types of vehicles by simply modifying the vehicle profile parameters as the vehicle dynamics remain the same. For instance, delivery trucks can be simulated by treating bus stops as delivery locations, or in the case of mining vehicles, the stops would correspond to loading of the vehicle or performing a work process such as concrete spraying or charging of explosives. In either case, the time spent at the stop can be freely set, and modelling of energy related to the work process can be included.

The torque of the electric motor is controlled by a proportional controller to make the vehicle follow the speed set point. The forces acting on the vehicle, i.e. aerodynamic drag, rolling resistance and gravitational force, are obtained from a longitudinal vehicle dynamics model. The powertrain is modelled by efficiency factors in order to keep the computation time short. The efficiency of the electric motor is dependent on the speed and torque, while the efficiencies of the inverter are considered constant. The battery is modelled as a constant voltage source with an internal resistance in order to include the influence of losses depending on the discharging and charging power. In addition to the energy required for the motion of the vehicle, energy consumed by auxiliary systems is drawn from the battery.

[72] Ranta, M. et al., 2016. Method Including Power Grid Model and Route Simulation to Aid Planning and Operation of an Electric Bus Fleet, VPPC, Hangzhou, China

For the purpose of vehicle fleet simulation, the charging process needs to be modelled as several vehicles share the same charging infrastructure. This can be achieved by modelling chargers as separate objects located at selected stops. Each charger is defined by a maximum power that can be drawn from the grid and a maximum number of vehicles that can charge simultaneously. When a vehicle comes to a charging station, it reserves a charging node if there is a free charging node available at the station. Connection to the charger (either manual or automatic) and initialization of the charging is modelled by adding a dead time to the charging session before the actual charging can start. The charging power is determined by the battery capacity and state of charge. The maximum power is used only at the beginning of the charging session, and the power decreases as the battery state of charge increases. When the battery state of charge reaches a predefined maximum value, charging stops and the charging node is free for the next vehicle to use. In this manner, interaction between vehicles at the charging station is taken into account, and the simulation can easily be extended to any number of vehicles and routes. An example simulated fleet can be seen in Figure 52.

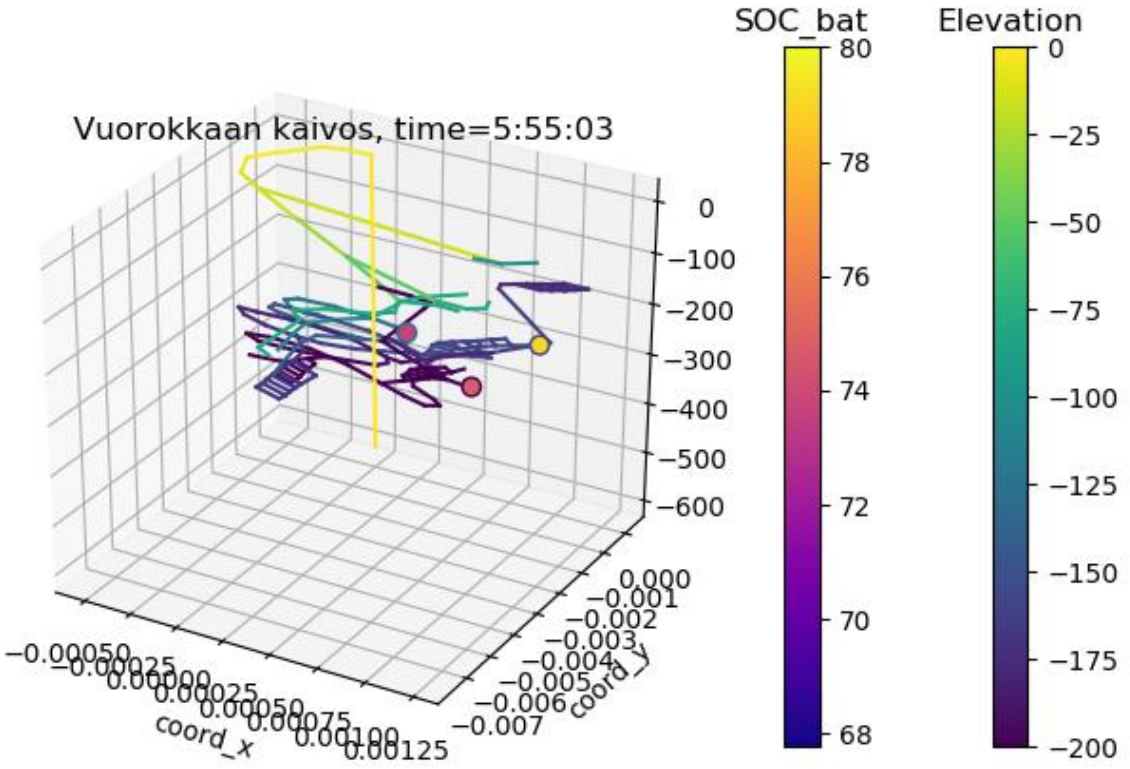


Figure 52. Visualization of a simple fleet of electric mining vehicles and their state of charge (SOC).

In addition to energy consumption computation, cost analysis is also of great importance for evaluating the performance of an electric vehicle fleet. A total cost of ownership (TCO) analysis comprises the relevant capital costs arising from owning a vehicle fleet: purchase of the vehicles, battery and charging infrastructure. The operational costs arise from energy as well as service and maintenance. Furthermore, each of the components (vehicle, battery, chargers) have their own service life (depreciation time) that has to be taken into account. A TCO module has been included in order to obtain the costs of the system in parallel to the energy consumption simulation. The module gives the costs of operation for one day, i.e. the capital costs are allocated to one day. For the case of charger investments, the costs are assumed to be dependent on the installed charging power and the charger lifetime is considered as constant. The cost of the batteries is a part of the capital costs, but the cost

also depends on the operation as the battery lifetime is dependent on the variation in the state of charge. In most cases, the vehicle depreciation time is rather long, and the battery has to be replaced at least once during the vehicle lifetime. Therefore, the batteries are treated separately from the vehicle investment costs. The battery lifetime is evaluated based on the variation of the battery state of charge during the simulated time frame using the rainflow algorithm. In this manner, the lifetime of the battery for three different battery chemistries (LFP, LTO and NMC) have been implemented.

The electricity costs are evaluated each time the battery is charged based on the charged amount of energy and the cost of electricity. The electricity cost is assumed to be dependent on the energy amount and the peak power is not assumed to affect the resulting cost, although this could be included. In addition to electricity costs, the salary costs for the drivers are included. Each vehicle requires a driver, and the more vehicles required to keep up the service level, the higher the salary expenses will be.

Optimization of an electric vehicle system is a demanding task due to the complexity and nonlinearity of such systems. The system cannot easily be linearized without losing critical information. Therefore, an optimization algorithm is implemented where the simulated system can be used as a cost function. Various techniques could be utilized for the purpose; within the TecNetwork project a methodology based on particle swarm optimization[73] has been implemented. The idea of the optimization is to find the best fleet for a specific case, i.e. to define the optimal battery capacity, battery type, charging power, charging locations and number of chargers at each location for a vehicle fleet. The methodology is flexible in the sense that the list of variables included in the optimization can easily be extended to also include features other than the ones mentioned here. The algorithm is designed to accept both continuous- and discrete-valued variables; for instance, the charging power is allowed to vary freely within certain limits while the battery chemistry naturally has to be treated as a discrete variable.

The optimization process starts with initialization of a swarm constituting a desired number of particles. Here, each particle corresponds to a solution set for the vehicle fleet. The variables are initialized randomly within the given search space, and each variable is randomly assigned an initial location and velocity. Each particle is evaluated by simulating the vehicle fleet with the given variables, i.e. with the given batteries and charging infrastructure. The fitness of the particle equals the resulting costs of the system based on the simulation. When all particles are evaluated, the locations and velocities are updated. Each particle moves towards both the global best (best position ever obtained by any particle in the swarm) and

Summary of the particle swarm optimization algorithm:

1. Initialization of swarm
   Each particle obtains a random position and random initial velocity
2. Evaluation of particles
   Simulations with settings corresponding to each particle, i.e. battery capacity, charging power, charging locations
3. Update personal best for each particle
4. Update global best
5. Calculate new velocities
6. Update particle positions
7. Repeat from step 2 until convergence criteria is met

[73] Khanesar, M. A., Teshnehlab, M. and Shoorehdeli, M. A., 2007, A Novel Binary Particle Swarm Optimization, Mediterranean Conference on Control and Automation, Athens, Greece

personal best position. An inertia is added to the velocity to avoid premature convergence in a local minimum, i.e. each particle tries to explore as much as possible of the search space. An example of the optimization process is shown in Figure 53.

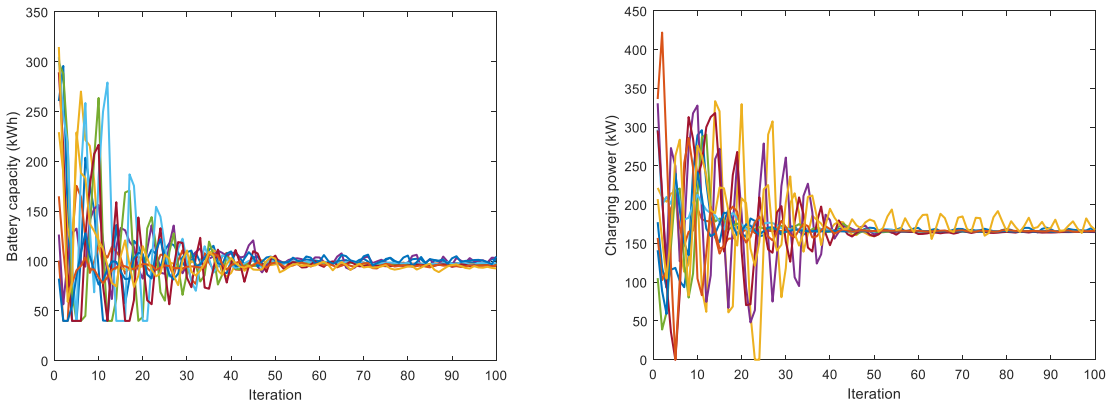


Figure 53. Example of evolution of battery capacity and charging power during the optimization process; 10 particles have been evaluated over 100 iterations.

7. Summary

The Tecnetwork project targeted at improving the productivity of industrial processes by creating new technological capabilities in selected most potential areas and considering cost-efficiency, availability performance, safety and smart decisions through the asset lifecycles.

The research results of the project will support machine and production system providers in creating new offerings with safer and sustainable processes, meeting the changing requirements of the business environment. This will require multi-disciplinary expertise from a number of partners in the future. The technological progress and the observations made from ecosystem level work will foster the creation of novel service offerings.